ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARININ DENETİMİ, DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN DENETİM REHBERİ ÖNERİSİ

Yasin BAKIRCI

UZMANLIK TEZİ

TELEKOMÜNİKASYON KURUMU

OCAK 2007

ANKARA

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-006-1

BTK Yayın No T 0125

Yasin BAKIRCI tarafından hazırlanan ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARININ DENETİMİ, DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN DENETİM REHBERİ ÖNERİSİ adlı bu tezin Uzmanlık tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Aydın GÜLAN
Tez Yöneticisi

Bu çalışma, jürimiz tarafından Telekomünikasyon Kurumu Uzmanlık tezi olarak kabul edilmiştir.

Başkan :

Üye :

Üye :

Üye :

Üye :

Üye :

Üye :

Bu tez, Telekomünikasyon Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICILARININ DENETİMİ, DÜNYA UYGULAMALARI VE TÜRKİYE İÇİN DENETİM REHBERİ ÖNERİSİ

(Uzmanlık Tezi)
Yasin BAKIRCI

TELEKOMÜNİKASYON KURUMU

OCAK 2007

ÖZET

Bu çalışmada, ESHS'lerin denetimine ilişkin usul ve esasları düzenleyen denetim mevzuatına ve Denetim Rehberine ilişkin öneriler ele alınmıştır. Elektronik imza ve denetim kavramları temel olarak açıklanmıştır. 99/93/EC sayılı Avrupa Birliği Direktifinde yer alan düzenlemeler ile farklı ülke örnekleri ESHS'lerin denetimi çerçevesinde incelenmiştir. Türkiye'de faaliyet gösteren ESHS'lerin denetimine ilişkin usul ve esaslar üzerinde durulmuştur. İncelemeler sonucunda, denetime ilişkin Telekomünikasyon Kurumu mevzuatında yer alan hükümlerin geliştirilmesi, Denetim Rehberinin hazırlanması ve uygulanması, denetim çalışmalarının periyodik olarak yapılması, elektronik imza mevzuatı çerçevesinde ihtiyari akreditasyon konusunun düzenlenmesi ve sertifika hizmeti sağlayan kamu kurum ve kuruluşlarına ilişkin denetim muafiyetinin sınırlandırılması gerektiği değerlendirilmiştir.

Anahtar Kelimeler : Denetim Rehberi, ESHS, elektronik imza, denetim

Sayfa Adedi : 151

Tez Yöneticisi : Doç. Dr. Aydın GÜLAN

SUPERVISION OF ELECTRONIC CERTIFICATE SERVICE PROVIDERS, WORLD PRACTICES AND SUPERVISION GUIDE PROPOSAL FOR TURKEY

(Telecommunications Expert Thesis)

Yasin BAKIRCI

TELECOMMUNICATIONS AUTHORITY

JANUARY 2007

ABSTRACT

In this study, proposals regarding supervision legislation that define rules and procedures about supervision of ECSPs and Supervision Guide have been evaluated. Electronic signature and supervision concepts have been examined basically. European Union Directive 1999/93/EC regulations and experiences of different countries have been assessed within the framework of supervision of ECSPs. The supervision rules and procedures regarding ECSPs established in Turkey have been assessed. As a result of the analysis, it is considered that supervision regulations in Telecommunications Authority legislation should be improved, Supervision Guide should be prepared and implemented, supervision works should be done periodically, voluntary accreditation issue should be regulated within the framework of electronic signature legislation and the supervision exemption of public entities and establishments providing certification services should be limited.

Key Words : Supervision Guide, ECSP, electronic signature, supervision

Page Number : 151

Advisor : Assoc. Prof. Aydın GÜLAN

TEŞEKKÜR

Çalışmam boyunca, yönlendirici ve yol gösterici olan ve değerli görüş, öneri ve deneyimlerini benden esirgemeyen tez danışmanım Sn. Doç. Dr. Aydın GÜLAN'a, tezin nihaî hale gelmesinde olduğu kadar mesleki yaşamımda da bilgi ve deneyimlerinden yararlandığım Daire Başkanım Sn. Mustafa ÜNVER'e, kıymetli görüş ve değerlendirmeleriyle tez çalışmalarım sırasında bana ufuk açan Daire Başkanım Sn. İhsan KULALI'ya, Köksal ÖZENÇ'e, Kuddusi YAZICI'ya, Cengiz EKEN'e ve Cafer CANBAY'a, maddi ve manevi desteğini her zaman hissettiğim sevgili eşime, anneme, babama ve dostlarıma teşekkür ederim.

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

KISALTMALARIN LİSTESİ

AAA	Açık Anahtar Altyapısı
AICPA	American Institute of Certified Public Accountants (Amerikan Yeminli Serbest Muhasebeciler Enstitüsü)
BNetzA	Federal Network Agency for Electricity, Gas, Telecommunications, Postal Service and Railways (Almanya Federal Elektrik, Gaz, Telekomünikasyon, Posta Hizmetleri ve Demiryolları Ağı Kurumu)
B2B	Business to Business (İşten işe)
B2C	Business to Costumer (İşten Müşteriye)
BGİ	Bilgi Güvenliği İlkeleri
BSI	Bundesamt für Sicherheit in der Informationstechnik (Bilgi Teknolojileri Güvenlik Bürosu)
CIBG	Central Information Point- Health Care Professionals (Merkezi Bilgi Noktası- Sağlık Bakım Profesyonelleri)
CWA	CEN Workshop Agreement (CEN Çalıştay Kararı)
Direktif	99/93/EC sayılı Avrupa Birliği Direktifi
DSA	Digital Signature Algorithm (Sayısal İmza Algoritması)
EA	European Co-oparation for Accreditation (Avrupa Akreditasyon İşbirliği)
EAL	Evaluation Assurance Level (Değerlendirme Garanti Düzeyi)
ECP.NL	Electronic Commerce Platform of the Netherlands (Hollanda Elektronik Ticaret Platformu)

EPDK	Enerji Piyasası Düzenleme Kurumu
ESHS	Elektronik Sertifika Hizmet Sağlayıcısı
ETSI TS	European Telecommunications Standards Institute Technical Specification (Avrupa Telekomünikasyon Standartları Enstitüsü Teknik Özellikleri)
FESA	Forum of European Supervisory Authorities for Electronic Signatures (Avrupa Elektronik İmza Denetim Kurumları Forumu)
FIPS	Federal Information Processing Standards Publications (Federal Bilgi İşleme Standartları Yayınları)
GPS	Global Positioning System (Küresel Konum Bulma Sistemi)
IAF	International Accreditation Forum (Uluslararası Akreditasyon Forumu)
IETF RFC	Internet Engineering Task Force Request for Comments (İnternet Mühendisliği Görev Grubu Yorum Talebi)
ISO	International Organisation for Standardisation (Uluslararası Standardizasyon Teşkilatı)
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commitee (Uluslararası Standardizasyon Teşkilatı/Uluslararası Elektroteknik Komitesi)
ITSEC/CC	Information Technologies Security Evaluation Criteria/Common Criteria (Bilgi Teknolojileri Güvenlik Değerlendirme Kriterleri/Ortak Kriterler)
ITU-TRec.	International Telecommunications Union – Telecommunications Standardization Sector Recommendation (Uluslararası Telekomünikasyon Birliği – Telekomünikasyon Standardizasyon Sektörü Tavsiyesi)
Kanun	5070 sayılı Elektronik İmza Kanunu

KCAC	Korea Certification Authority Central (Kore Merkezi Sertifikasyon Kurumu)
KISA	Korea Information Security Agency (Kore Bilgi Güvenliği Dairesi Başkanlığı)
KPMG	Klynveld Peat Marwick Goerdeler
LDAP	Lightweighted Directory Access Protocol (Hafifletilmiş Dizin Erişim Protokolü)
NCA	National Computerization Agency (Milli Bilgisayarlandırma Dairesi)
OCSP	Online Certificate Status Protocol (Çevrimiçi Sertifika Durum Protokolü)
OLAS	Office Luxembourgeois d'Accréditation et de Surveillance (Lüksemburg Akreditasyon Kurumu)
OPTA	Independent Post and Telecommunications Authority (Hollanda Bağımsız Posta ve Telekomünikasyon Kurumu)
PKIoverheid	Hollanda Devlet Açık Anahtar Altyapısı
RegTP	Regulatory Authority for Telecommunications and Posts (Almanya Telekomünikasyon ve Posta Düzenleyici Kurumu)
RSA	Rivest-Shamir-Adleman
RvA	Raad Voor Accreditatie (Hollanda Akreditasyon Konseyi)
SHS	Sertifika Hizmet Sağlayıcısı
Sİ	Sertifika İlkeleri
SPK	Sermaye Piyasası Kurulu
SUE	Sertifika Uygulama Esasları
SWEDAC	Swedish Board for Accreditation and Conformity Assessment (İsveç Akreditasyon ve Uygunluk Değerlendirme Kurulu)

T-Systems	Zertifizierungsstelle der T-Systems (T-Systems Sertifikasyon Merkezi)
Tebliğ	Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ
TK	Telekomünikasyon Kurumu
TSE	Türk Standartları Enstitüsü
TTP. NL	Trusted Third Party of the Netherlands (Hollanda Güvenilir Üçüncü Taraf)
TURKAK	Türk Akreditasyon Kurumu
TÜBİTAK – UEKAE	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
TÜVIT	TÜV Informationstechnik GmbH (TÜV Bilgi Teknolojileri A.Ş.)
UKAS	United Kingdom Accreditation Service (Birleşik Krallık Akreditasyon Hizmeti)
UNCITRAL	United Nations Commission on International Trade Law (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)
UTC	Coordinated Universal Time (Koordine Edilmiş Evrensel Zaman)
UZI	Unieke Zorgverleners Identificatie (Tekil Kimlik Doğrulama)
Yönetmelik	Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik
ZDİ	Zaman Damgası İlkeleri
ZDUE	Zaman Damgası Uygulama Esasları

1. GİRİŞ

Günümüzde geleneksel ve alışılmış iletişim yöntemlerinden, elektronik iletişim yöntemine doğru hızlı bir değişim yaşanmaktadır. Bilgi ve iletişim teknolojilerindeki hızlı değişim ve gelişim, hayatı her yönüyle etkilemekte, sosyal ve ekonomik alanlarda değişimler oluşturmakta ve ülkelerin ekonomik kalkınmasını etkileyen önemli bir faktör olarak karşımıza çıkmaktadır.

Elektronik ticaret ve elektronik devlet, geçtiğimiz yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel olarak dünya genelinde giderek yaygınlaşan kavramlardır. İnternetin hızlı bir şekilde gelişmesi ve yayılması, elektronik devlet ve elektronik ticaret uygulamalarını hızla arttırmıştır. Bu uygulamalar kaynakların etkin kullanımı, zaman ve mekâna bağımlılığın azalması, açıklık, şeffaflık, hesap verilebilirlik, katılımcılık, hizmet kalitesi ve verimlilik artışı gibi imkânlar sunmuştur. Hem kamu sektöründe hem de özel sektörde gerçekleştirilen elektronik uygulamalar ile ürün ve hizmetlerin topluma daha hızlı ve daha güvenli bir şekilde ulaştırılması sağlanmaktadır.

Elektronik devlet ve elektronik ticaret uygulamalarının ve bu uygulamalara yönelik talebin gelişebilmesinin en önemli koşulu, elektronik ortama olan güvenin artırılmasıdır. Bilgi güvenliği noktasında taşıdığı değer dikkate alındığında elektronik imzanın, elektronik ticaret ve elektronik devlet alanlarında kullanımının gerek ticari gerekse kamusal işlemlerin güvenliği açısından hayati önem taşıdığı görülmektedir. Elektronik imza, elektronik ortamda muhatapları kesin olarak tespit etmesi ve güvensizlik duygusunu ortadan kaldırması sebebiyle söz konusu uygulamaların güvenli bir şekilde gerçekleştirilmesinde büyük rol oynamaktadır.

Elektronik ortamda gerçekleştirilen işlemleri hukuki açıdan geçerli kılan elektronik imzaya ilişkin düzenlemelerin temel amaçları arasında, rekabete ve gelişmeye engel olan hususların mümkün olduğunca ortadan kaldırılarak ekonomik etkinliğin sağlanması bulunmaktadır. TK (Telekomünikasyon Kurumu) tarafından hazırlanan düzenlemelerin yürürlüğe girmesini müteakip, rekabet kurallarına uygun faaliyet gösterilmesinin temini başta olmak üzere farklı pek çok gerekçeyle nitelikli

elektronik sertifika pazarının sıkı bir şekilde denetlenmesi zarureti ortaya çıkmıştır. Nitelikli elektronik sertifika pazarına giren ESHS (Elektronik Sertifika Hizmet Sağlayıcısı)'lerin, bu düzenlemelere uygun olarak faaliyette bulunup bulunmadıklarının belirlenebilmesi için bundan sonra denetim ağırlıklı bir uygulamanın gerçekleştirilmesi gerekmektedir.

Bu yeni dönemde, düzenleyici ve denetleyici kurum olarak TK'ya düşecek en önemli görev, yapılan düzenlemelerin etkin bir şekilde hayata geçirilmesi çerçevesinde, uygulamaların takip edilmesi ve denetlenmesi olacaktır. Bu itibarla, ESHS'lerin güvenilir bir biçimde hizmet sağlamalarına ilişkin şartları devam ettirip ettirmediğinin etkin bir şekilde denetlenmesi bakımından, mevzuatta yer alan denetime ilişkin hükümlerin gözden geçirilmesi, ayrıca denetim çalışmaları sırasında Denetim Rehberi gibi denetim araçlarının uygulanması gerekmektedir.

Bu çalışmanın amacı; etkin ve verimli bir denetim çalışması ortaya koymak için gerekli olan "Denetim Rehberi"nin hazırlanmasına ve ESHS'lerin denetimine ilişkin usul ve esasları düzenleyen denetim mevzuatına ilişkin öneriler geliştirmektir.

Giriş bölümünü takiben ikinci bölümde; elektronik imza ve denetim kavramları hakkında temel bilgilere yer verilmiştir.

Üçüncü bölümde; SHS (Sertifika Hizmet Sağlayıcısı)'lerin denetimine ilişkin 99/93/EC sayılı Avrupa Birliği Direktifinde yer alan düzenlemeler ile denetim yapıları itibariyle farklılık gösteren Almanya, Hollanda ve Güney Kore örnekleri incelenmiştir.

Dördüncü bölümde; Türkiye'de faaliyet gösteren ESHS'lerin denetimine ilişkin usul ve esaslar anlatılmıştır.

Beşinci bölümde; ülkemizde faaliyet gösteren ESHS'lerin etkin ve verimli bir şekilde denetlenmesi açısından TK mevzuatında yer alan hükümler değerlendirilmiş, mevzuata ve Denetim Rehberinin oluşturulmasına ve uygulanmasına ilişkin öneriler sunulmuştur.

2. TEMEL BİLGİLER

2.1. Elektronik İmza Hakkında Temel Bilgiler

Geleneksel ve alışılmış iletişim yöntemlerinden elektronik iletişim yöntemine doğru hızlı bir değişim ve gelişimin yaşandığı günümüzde, elektronik ortama aktarılan işlemlerin ve iş akışlarının belirli güvenlik seviyesinde gerçekleştirilebilmesi açısından elektronik imza büyük önem taşımaktadır.

Elektronik imza, iki tarafın elektronik bir ortam üzerinden karşılıklı olarak kimliklerinden şüphe duymadan ve gönderilen veya alınan verilerin hiçbir şekilde değişmediğini bilerek haberleşmesini sağlamaktadır. Bu itibarla, elektronik devlet ve elektronik ticaret uygulamalarının gelişmesi ve kullanıcılar tarafından benimsenmesi için elektronik imzaya güven duyulmasını sağlamak gerekmektedir [1].

2.1.1. Elektronik imzanın tanımları ve işlevleri

Elektronik imza; gelişmiş teknolojiler kullanılarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun doğrulanmasını, iletilen veya alınan verilerin bilinen kişiler tarafından gönderildiğinin belirlenmesini, verileri gönderenlerin gönderdiğini ve alanların aldığını inkâr edememesini, gönderilen veya alınan bilgilerin içeriğinin değiştirilememesini, başkaları tarafından elde edilse bile, içeriğinin başkaları tarafından anlaşılamamasını garanti eden, elektronik ortamda bit[1] dizilerinden oluşturulmuş güvenli haberleşme ortamına verilen isim olarak nitelendirilmiştir [2].

Bir başka tanımda elektronik imza kavramı; sayısal imza ve sayısallaştırılmış imza gibi alt tanımları içermekle birlikte, genel olarak sayısal imzayı işaret etmektedir [3]. Sayısal imza ise, bir elektronik mesaj veya iletiye eklenen ve göndereni emsalsiz şekilde tanımlayan veya taklit edilmesi çok zor olan bir sayısal kod olarak tanımlanmaktadır [2].

---

[1] Bit, verinin en küçük birimidir. Tek bir ikili değere sahip olup, 0 veya 1 olabilir.

Bir başka kaynakta elektronik imza; elektronik bir ses, sembol veya veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan verileri değiştirmek veya işlemek için kişinin verileri imzalama girişimi olarak da tarif edilmektedir [4].

5070 sayılı Elektronik İmza Kanununun (Kanun) 3 üncü maddesinde ise elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan, kimlik doğrulama amacıyla kullanılan, inkâr edememe ve bütünlüğü sağlayan elektronik veriyi ifade etmektedir.

Kanunun 4 üncü maddesinde güvenli elektronik imza; münhasıran imza sahibine bağlı olan, güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya[2] dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza türü olarak tanımlanmıştır.

Yukarıda belirtilen tanımlar dikkate alındığında elektronik imza; kimlik doğrulama, gizlilik, bütünlük ve inkâr edememezlik işlevlerini haiz bulunmaktadır.

- Kimlik Doğrulama: Bir kullanıcının kendisine ait olduğunu iddia ettiği kimliğin doğrulanması ve onaylanmasıdır. Diğer bir deyişle, veriyi gönderen kişinin kimliğinin doğruluğundan emin olunması kimlik doğrulama işlevini tanımlamaktadır. Kimlik doğrulama işlevinde gizli anahtarın önemli bir rolü bulunmaktadır. Zira gizli anahtarın sadece ilgili kişiye ait olması ve gizli tutulması nedeniyle, yapılacak işlemlerin sadece söz konusu kişi tarafından

[2] Güvenli elektronik imzayı diğer elektronik imzalardan ayıran başlıca unsur nitelikli elektronik sertifikadır. Nitelikli elektronik sertifika, elektronik sertifikanın bir türüdür. Kanunun 3 üncü maddesinde elektronik sertifika, imza sahibinin imza doğrulama verisini (açık anahtar) ve kimlik bilgilerini birbirine bağlayan elektronik kayıt olarak tanımlanmaktadır. Diğer elektronik sertifikalardan farklı olarak, nitelikli elektronik sertifikanın içinde yer alması gereken bilgiler Kanunun 9 uncu maddesi kapsamında düzenlenmiştir. Elektronik sertifika, açık anahtarın kime veya neye ait olduğunu gösteren elektronik doküman olup, açık anahtar kullanılarak yapılan işlemlerin doğrulanabilmesini sağlamaktadır [14]. Elektronik sertifika, temelde en az ait olduğu kişinin ad ve soyadı ile açık anahtarını içermek durumundadır.

gerçekleştirilebileceği kabul edilmektedir. Gizli anahtarın yanında açık anahtarın ilgili kişiye ait olup olmadığının kontrolü de elektronik sertifika marifetiyle yapılmaktadır [1].

- Gizlilik: İletilen verilerin yetkisiz kişilerden gizlenmesi olarak tanımlanabilir. Güvenliğin en temel adımı olan gizlilik, şifre bilimi (kriptografi) ile sağlanır. Şifreleme; elektronik haberleşmede bilginin, üçüncü şahısların eline geçse bile, anlaşılamayacak veya çözümlenemeyecek bir şekile dönüştürülmesi işlemidir. Gönderilen ve/veya alınan şifreler bir şifreleme algoritması kullanılarak farklı bir formata dönüştürülmektedir. Bu sayede, üçüncü şahıslar farklı formata dönüştürülmüş olan gizlenmiş mesajları çözemeyecekleri için güvenli bir ortam oluşturulmuş olmaktadır [2].

- Bütünlük: Bir dokümanın veya mesajın içeriğinin değiştirilememesinin sağlanması olarak ifade edilmektedir [2]. İletilen verilerin doğruluğunun ve eksiksizliğinin sağlanması işlemidir. Gönderilen verinin özetleme algoritmasından geçirilerek özet değerinin hesaplanması ve çıkan sonuçların karşılaştırılması ile gerçekleştirilmektedir [5].

- İnkâr Edememezlik: Veriyi gönderen veya işleyen kişinin yaptığı işi sonradan inkâr edememesidir [6]. Elektronik imzanın, kişilerin elektronik ortamda gerçekleştirdikleri işlemleri inkâr etmelerini önleme işlevi bulunmaktadır [7].

2.1.2. Elektronik imzanın uygulama alanları

Farklı seviyelerde güvenlik sağlayabilen elektronik imza, birçok alanda uygulanabilmektedir. Elektronik imza kimlik tanımlama, doğrulama ve veri paylaşımı gibi uygulamalarda kullanılabileceği gibi, milli güvenlikten kişisel güvenliğe; elektronik ticaretten mobil ticarete; B2B (Business to Business-İşten işe)'den, B2C (Business to Costumer-İşten Müşteriye)'ye; güvenli elektronik posta, elektronik banka ve güvenli bilgisayar erişimleri oluşturmaya kadar birçok alanda uygulama sahası bulabilmektedir [2].

Elektronik imzanın; bankalar ve finans kurumları, sigorta şirketleri, kamu kurum ve kuruluşları, holdingler ve diğer büyük şirketler, üniversiteler, iletişimde en üst seviyede bilgi güvenliği gereksinimi olan organizasyonlar bağlamında yaygın bir uygulama alanı bulabileceği değerlendirilmektedir [3].

Aşağıda, gerek kamusal gerekse ticari alanda görülen ve görülmesi muhtemel olan elektronik imza uygulamaları sıralanmaktadır [8].

Kamusal Alandaki Uygulamalar:

- Her türlü sınav başvuruları,
- Kurumlararası iletişim,
- Sosyal güvenlik uygulamaları,
- Sağlık uygulamaları (Sağlık personeli, hastaneler, eczaneler),
- Vergi ödemeleri,
- Belediye işlemleri (Su, gaz, temizlik, ihale vb.),
- Elektronik oy verme işlemleri.

Ticari Alandaki Uygulamalar:

- Bankacılık işlemleri,
- Sigortacılık işlemleri,
- Elektronik sözleşmeler,
- Elektronik siparişler.

2.2. Elektronik İmzanın Teknik Altyapısı

Elektronik imza, AAA (Açık Anahtar Altyapısı) kullanılmak suretiyle, imzalama ve doğrulama aşamalarından oluşmaktadır. Elektronik imzalama ve doğrulama süreçlerinin yanında AAA, şifreleme, özetleme algoritması, imza oluşturma ve doğrulama araçları ile zaman damgası gibi kavramlar açıklanacaktır.

2.2.1. Şifreleme

İnsanların iletişime geçmesiyle birlikte, iletişim kaynaklarının istenmeyen alıcılardan korunmasına yönelik gelişen ihtiyaç çerçevesinde, veri saklanmasına ilişkin sayısız yöntem geliştirilmiştir. Bir kısım yöntemler; harflerin, kelimelerin veya bitlerin anlaşılmaz ifadelere çevrilmesine yönelik olmuştur. Bu yöntemler ile, veri alıcısı konumunda bulunan kişinin veriyi gönderen kişiye ait mesajı okuyabilmek için kendisine gönderilen anlaşılmaz ifadeleri asıl şekline dönüştürebilmesi, söz konusu veriye erişime yetkili olmayan kişilerin anlaşılmaz ifadelerden mesajın asıl şekline ilişkin herhangi bir çıkarım yapamaması amaçlanmıştır. Yukarıda belirtilen amaçları gerçekleştiren ve en yaygın kullanımı haiz olan yöntem şifreleme yöntemidir [26].

Şifreleme; bilgi güvenliğini sağlama noktasında işlev gören matematiksel teknikler bütünüdür. Şifreleme ile, ilgili olmayan kişilerin gönderilen verileri elde etmesi önlenmektedir [9]. Güvenlik düzeyi, işlevsellik, işlem metotları, performans ve kolay uygulanabilirlik gibi değerlendirme kıstasları, güvenli olmayan kanallar üzerinden haberleşmede veya verilerin güvenli olmayan ortamlarda saklanmasında kullanılan şifreleme açısından büyük önem taşımaktadır [10].

Şifreleme anahtar vasıtasıyla yapılmaktadır. Şifreleme ve şifre çözmede kullanılan, genelde rastgele bitlerden oluşan sayı dizisine anahtar denir [3]. Anahtar, verilerin işleme tabi tutularak anlaşılmaz hale sokulduğu daha sonra ise tekrar anlaşılabilecek duruma getirildiği yani deşifre edildiği algoritmaya dayanan formüldür. Şifreleme için tek bir anahtar kullanılabildiği gibi çift anahtar da kullanılabilmektedir [11].

Literatürde "anahtar çifti" ifadesi yerine açık anahtar ile özel veya gizli anahtar ifadeleri kullanılmaktadır. 99/93/EC sayılı Avrupa Birliği Direktifinde (Direktif) geçen kavramlara uygun olarak Kanunda, *imza oluşturma verisi* ve *imza doğrulama verisi* kavramlarına yer verilmiştir. Kanunun 3 üncü maddesinde imza oluşturma verisi; imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik *gizli anahtarlar* gibi verileri, imza doğrulama verisi ise elektronik imzayı doğrulamak için kullanılan

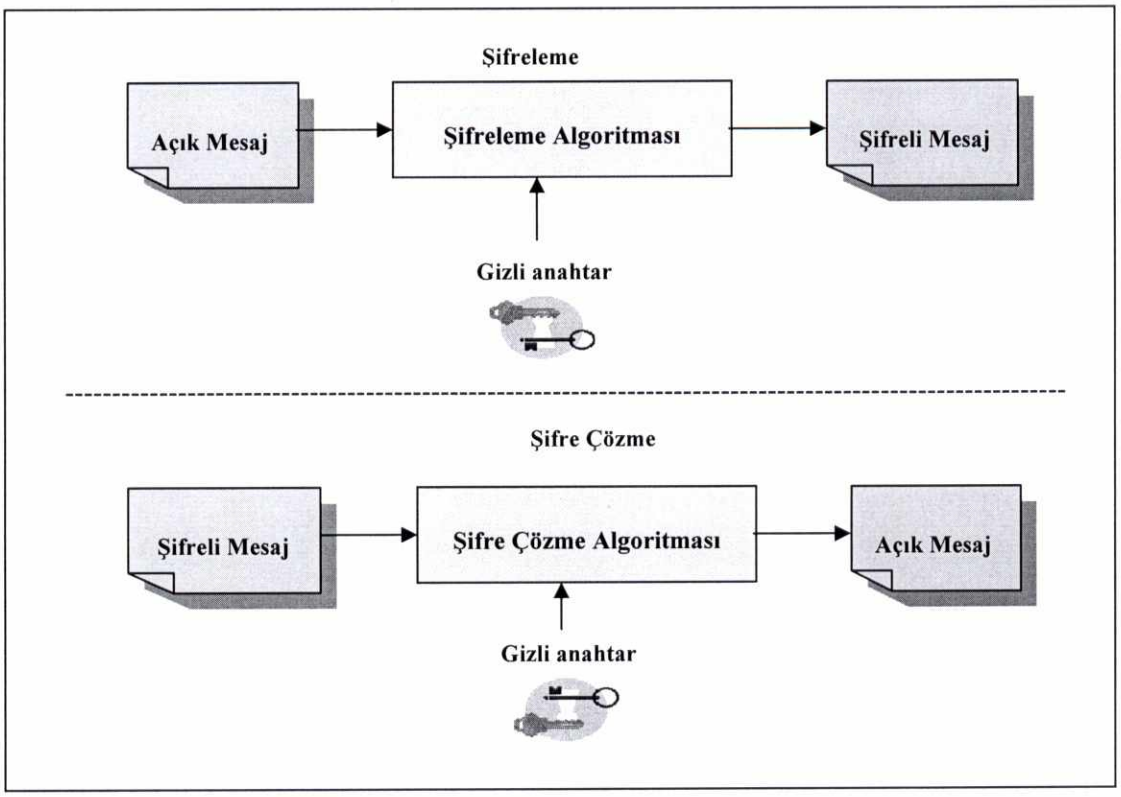
şifreler, kriptografik *açık anahtarlar* gibi verileri ifade etmektedir. Bu çalışmada, kullanım kolaylığı dikkate alınarak, imza oluşturma verisi kavramı yerine *"gizli anahtar"*, imza doğrulama verisi kavramı yerine ise *"açık anahtar"* kavramları kullanılacaktır.

Yüzyıllardır süregelen gelişmeler ışığında büyük değişim gösteren şifreleme teknikleri, kullanılan anahtarlar temel alınarak *simetrik şifreleme* ve *asimetrik şifreleme* olarak iki ana başlıkta incelenebilir.

2.2.1.1. Simetrik şifreleme

Simetrik şifreleme, hem şifreleme hem de şifre çözme işlemi için aynı anahtarın kullanıldığı uygulamalardır. Aynı anahtarın kullanılması, hem göndericinin hem de alıcının bu anahtarı bilmesi anlamına gelmektedir [12]. Gönderici ve alıcı, iletişimi güvenli bir şekilde gerçekleştirmek için bir gizli anahtar üzerinde uzlaşmaktadır. Seçilen gizli anahtar ile mesajlar veya açık metinler şifrelenmekte veya şifrelenmiş mesajların ve açık metinlerin şifreleri çözülebilmektedir. Birbiri ile şifreli haberleşmek isteyen taraflar, gizli anahtarı paylaşmak zorundadır [1],[2]. (Şekil 2–1)

Simetrik şifreleme yöntemi, hızlı çalışma ve algoritmaların donanımla kolay gerçeklenebilmesi gibi avantajlara sahiptir. Ancak simetrik şifreleme; anahtar yönetiminin zor olması, gizli anahtarı paylaşma zorunluluğu, tanınmayan kişilerle haberleşmede meydana gelebilecek zorluklar, bütünlük ve kimlik doğrulamanın tam anlamıyla uygulanamaması gibi dezavantajları da beraberinde getirmektedir [6].



Şekil 2–1: Simetrik şifreleme

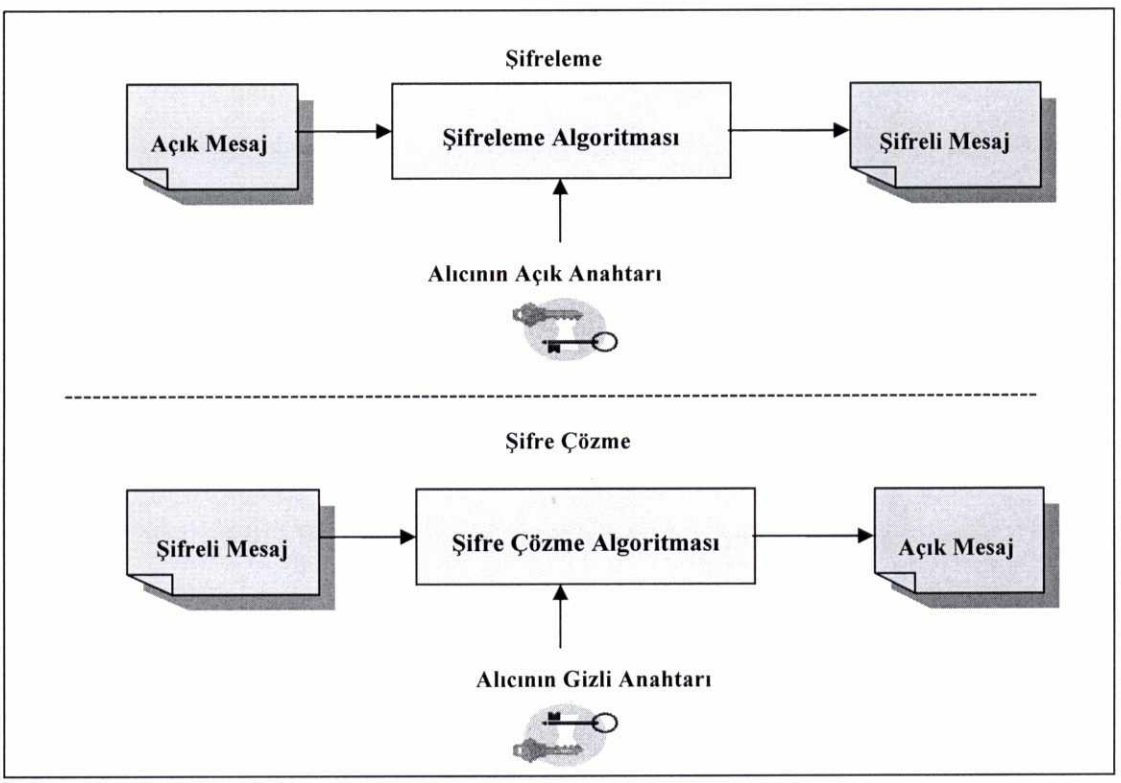
2.2.1.2. Asimetrik şifreleme

Asimetrik şifrelemede, şifreleme ve şifre çözme işlemleri için matematiksel olarak ilişkili, fonksiyonel olarak birlik içinde [13], fakat birbirinden farklı anahtarlar kullanılmaktadır. Bu anahtarlar çift olarak üretilmekte, tek yönlü çalışmakta ve birbirlerini tamamlamaktadır. Şifreleme işlemi açık anahtar ile, şifre çözme işlemi ise gizli anahtar ile yapılmaktadır. Bu bakımdan asimetrik şifreleme, açık anahtar şifrelemesi olarak da nitelendirilmektedir [14].

Açık anahtar şifreleme işleminde, açık anahtar ile şifrelenen açık mesajların şifresi yalnız gizli anahtar kullanılarak çözülebilmektedir. Gizli anahtar sadece sahibi tarafından bilinmekte ve anahtar sahibi göndereceği verileri bu anahtar ile şifrelemektedir. Gizli anahtar yalnızca gönderici kişide olduğundan, gizli anahtarla şifrelenmiş bir mesaj, o kişinin alıcıdaki açık anahtarı ile uyumlu olması durumunda

göndericinin kimliği onaylanmış olmaktadır. Bu durum, bir kişinin, başka birisinin kimliğini kullanarak işlem yapmasını engellediği gibi, gönderenin yaptığı işlemi inkâr etme ihtimalini de büyük ölçüde ortadan kaldırmaktadır. Açık anahtarı ise, sahibinin lüzum gördüğü herkes bilebilmekte ve bu anahtar, gizli anahtar ile şifrelenmiş olan metnin şifresini çözmek için kullanılmaktadır.

Örnek olarak, alıcıya gizli bir mesaj göndermek isteyen gönderici, alıcının açık anahtarıyla mesajı şifreler ve gönderir. Şifrelenmiş bu mesajın şifresi, yalnızca açık anahtara karşılık gelen gizli anahtara sahip olan kişi tarafından çözülerek okunabilir. (Şekil 2–2)



Kaynak: [15]

Şekil 2–2: Asimetrik şifreleme

Açık ve gizli anahtar birbirleriyle ilişkili oldukları halde açık anahtardan gizli anahtara ulaşmak veya tersi bir durum, büyük bir işlem gücü gerektirdiğinden dolayı, neredeyse imkânsızdır. Asimetrik şifreleme; anahtar yönetiminin kolay olması ve

algoritmaların kırılmaya karşı daha dirençli olmaları gibi avantajlara sahiptir. Ancak asimetrik şifreleme, simetrik şifrelemeye göre oldukça yavaş çalışmakta ve kullanılan anahtarlar bazı uygulamalarda sorun oluşturabilecek kadar uzun olmaktadır [1].

2.2.2. Özetleme algoritması

Farklı uzunluklarda mesaj, doküman veya yazıyı işleyerek sabit uzunlukta veri oluşturma işlemine özetleme denir. Özetleme algoritması, girdi olarak kullanılan herhangi bir uzunluktaki veriyi işleyerek sabit uzunlukta bir özet değeri üreten tek yönlü algoritmadır. Özetleme algoritmasının en önemli özelliği, birbirinden çok az farklı girdiler için dahi tamamen ayrı çıktılar üreterek çakışmaları önleyebilmesidir. (Çizelge 2–1)

Özetleme algoritması, elektronik imzanın hazırlanması için son derece önemlidir. Zira özet değerleri, veri bütünlüğünün bozulup bozulmadığını kontrol etmek için kullanılmaktadır. Hazırladığı mesajı imzalamak isteyen kimse, mesajının özetleme değerini hesaplamak için bir özetleme algoritması kullanmaktadır. Bu şekilde özetleme değeri, gizli anahtar ile şifrelenmiş olmaktadır. Bir belgenin özetleme değeri belli olduğu için, alıcı bunu mesajı gönderenin açık anahtarı yardımıyla tespit edebilmektedir. Alıcı, özetleme algoritmasını bu defa deşifre edilen mesaja da uygulayabilmekte ve her iki değeri birbiri ile karşılaştırabilmektedir.

Her iki değer birbirine uyuyorsa, alıcı, bu belgenin göndericinin asıl belgesi olduğundan ve mesajın sonradan değiştirilmediğinden emin olabilmektedir [16]. Mesajın sonradan değiştirilmesi halinde, elde edilen özetleme değerleri birbirinden farklı olmaktadır.

Çizelge 2–1: Özetleme algoritması

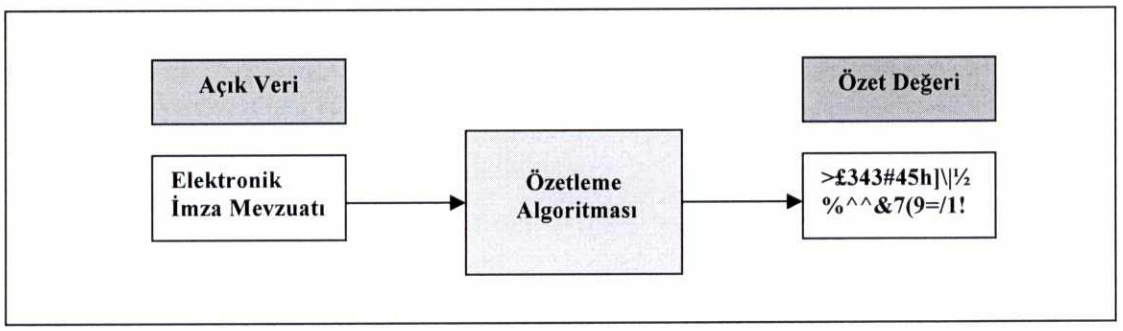
Giriş Mesajı	Özet Değeri
Elektronik İmza Mevzuatı	53AC528CA6033654A84A3E456D3214 84A3E456D321453AC528CA684A3E44
Elektrunik İmza Mevzuatı	33654A84A3E456D32144A3E456D3E2 821453AC528CA684A3E4453AC5286
Farklı uzunluklarda mesaj, doküman veya yazıyı işleyerek, oluşturma işlemine özetleme denir.	21453AC56D32144A3E456D3E228CA 684A3E448553AC528633654A84A3E4

2.2.3. Elektronik imzalama ve doğrulama

Elektronik ortamda gönderilen mesaj veya dokümanlar genelde *açık mesaj* olarak adlandırılır. Elektronik ortamda mesaj içeriklerinin gizlenmesi veya kolaylıkla algılanamayacak bir şekle dönüştürülmesi hususunda işlev gören şifreleme işlemi ile mesaj güvenli olarak iletilse de tam bir güvenlik için şifreleme yeterli değildir. Şifreleme işlemine ek olarak; kimlik doğrulama, bütünlük ve inkâr edememezlik gibi işlevlerin de haberleşme sırasında sağlanması gerekmektedir.

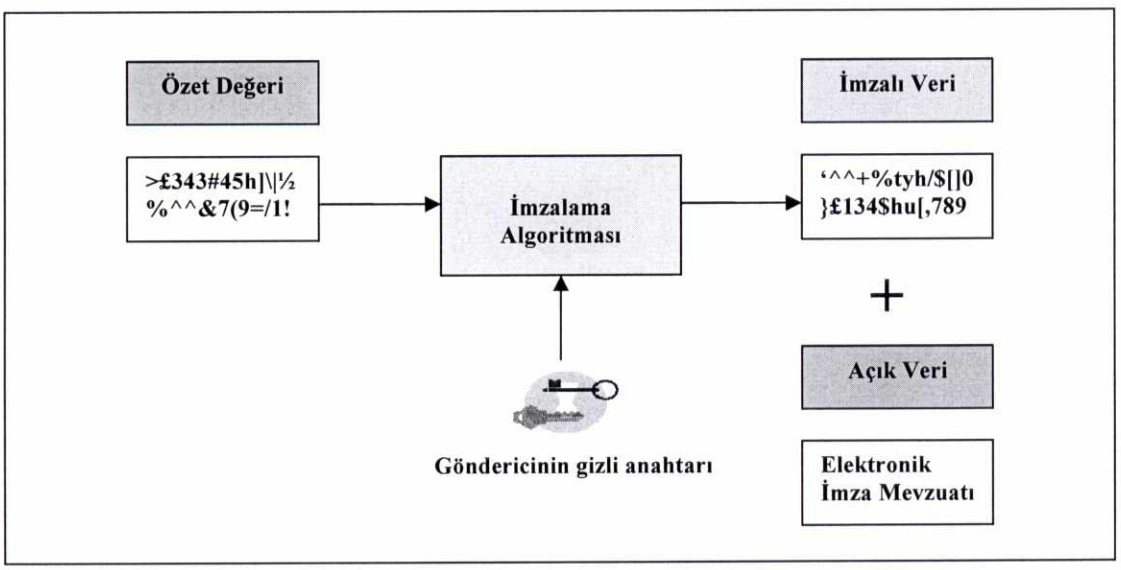
Söz konusu işlevlerin işler hale geldiği imzalama ve doğrulama işlemleri aşamalar halinde aşağıda açıklanmıştır. Birinci ve ikinci aşamalar imzalama yapan kişi tarafında, üçüncü aşama ise doğrulama yapan kişi tarafında gerçekleşmektedir.

Birinci Aşama: Şekil 2–3'de "Elektronik İmza Mevzuatı" ifadesi imzalanacak veri olarak gösterilmektedir. Söz konusu veriye özetleme algoritması uygulanır ve böylelikle sabit uzunlukta olan bir özet değeri elde edilir. Veri bütünlüğünün kontrolünde, gönderilecek verinin yüksek hacimde olması durumunda ve imzalama süresini kısaltmada özet değerinin alınması işlemi oldukça önemli bir rol oynamaktadır.



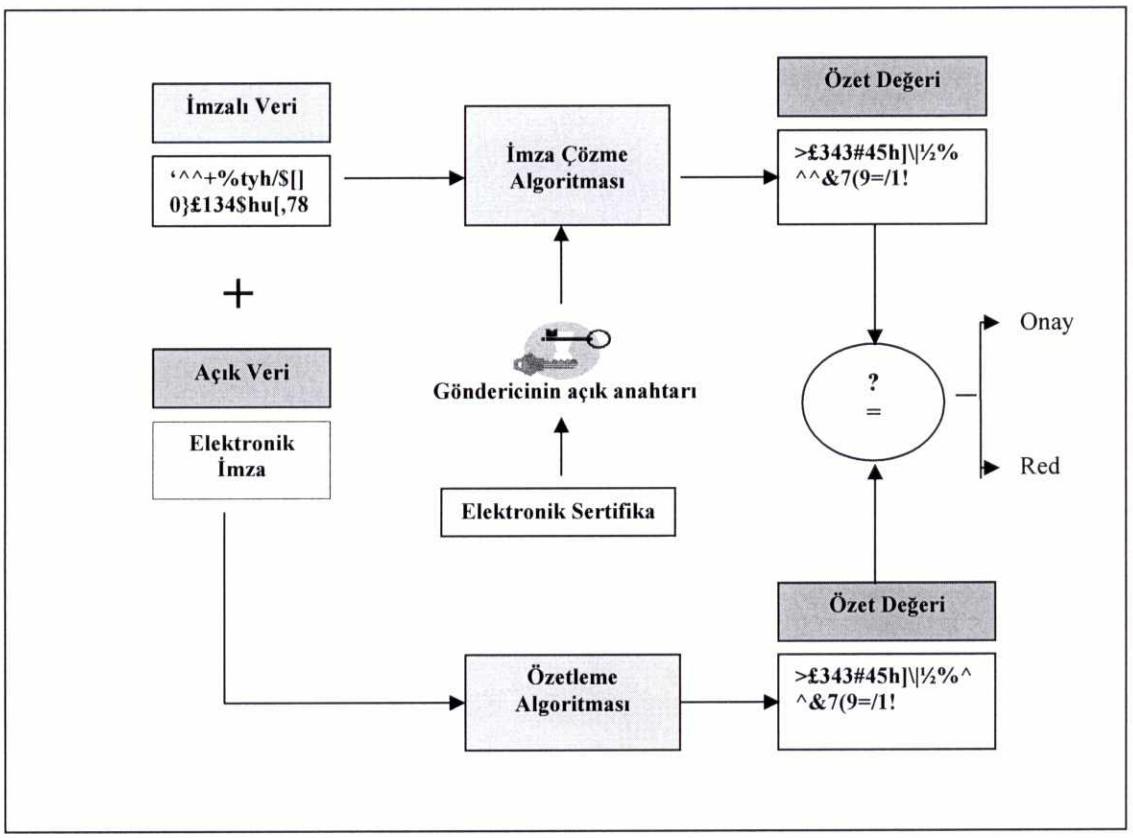
Şekil 2–3: Elektronik imzalama (Birinci aşama)

İkinci Aşama: İmzalanacak veriye uygulanan özetleme algoritması ile elde edilen özet değeri, imzalama yapacak kişinin (göndericinin) gizli anahtarı ile şifrelenir ve imzalanan verinin aslı ile birlikte alıcıya gönderilir. (Şekil 2–4)



Şekil 2–4: Elektronik imzalama (İkinci aşama)

Üçüncü Aşama: Alıcı, kendisine gelen imzalanmış veriyi, göndericinin elektronik sertifikasında bulunan açık anahtar ile çözer. Ayrıca imzalanan verinin aslına özetleme algoritması uygulanarak özet değeri bulunur ve söz konusu veri imzalanan özet değeri ile karşılaştırılır. Gerçekleşen doğrulama işlemi sonucunda, iki özet değeri arasında herhangi bir farklılık olması mesaj bütünlüğünün bozulduğunu gösterir [17]. (Şekil 2–5)



Şekil 2–5: Elektronik imzada doğrulama

Üçüncü aşamada alıcı, kendisine gelen imzalanmış veriyi, göndericinin elektronik sertifikasında (açık anahtar sertifikası) bulunan açık anahtar ile çözmektedir.

Elektronik sertifikanın ve sertifika içerisinde yer alan bilgilerin doğruluğundan emin olunabilmesi için güven hiyerarşisi kurulmalıdır. Bir başka ifadeyle, yayınlanan sertifikaların, güvenilir kuruluşlar yani SHS'ler tarafından elektronik olarak imzalanmış olması gerekmektedir. Bu yapıda hiyerarşinin en üst noktasında bulunan SHS, sertifikasını kendisi imzalamaktadır. Bu mekanizma ile herhangi bir kişinin başkası adına sertifika oluşturmasının ve sertifikaları tahrif etmesinin önüne geçilmektedir [1].

2.2.4. Açık anahtar altyapısı

AAA, belli bir kullanıcı topluluğu için açık anahtar teknolojisinin işlemesine izin veren organizasyonların, sistemlerin (yazılım-donanım), süreçlerin, ilkelerin ve sözleşmelerin toplamına verilen addır. "Açık Anahtar Altyapısı" ifadesi içindeki "altyapı" kavramı, aynı zamanda genel uygulamaların[3] ve iş uygulamalarının[4] güvenli bir şekilde hayata geçirilebileceği ve işleme konabileceği bir altyapıyı veya oluşumu tanımlamaktadır [20].

Yukarıda belirtilen tanımların yanında, AAA, *"açık anahtar şifrelemesi üzerine kurulmuş güven zinciri"* [21] veya *"internet kullanıcılarının aralarında güvenli ve gizli iletişimi sağlayan kapsamlı sistem ilkeleri, süreçleri ve teknolojilerin birlikte çalıştığı uygulamalar bütünü"* olarak da tanımlanmaktadır [22].

Elektronik ortamda verilerin güvenliği; bilgilerin güvenli olarak gönderilmesi ve/veya alınması, gizlilik, bütünlük, kimlik doğrulama ve inkâr edememezlik gibi işlevler ile sağlanmaktadır. Bu işlevleri gerçekleştirmek için güvenilir birimlere, şifreleme mekanizmalarına, güncel donanımların ve yazılımların kullanılmasına, farklı bit uzunluklarına sahip anahtarların seçimine ve bunların işleyişini sağlayan bilgisayar altyapısı ile uyulması ve denetlenmesi gereken uluslararası kurallara, standartlara ve ilkelere ihtiyaç bulunmaktadır.

Elektronik imzayı ve özellikle AAA'yı kullanan iletişim sistemlerinin teknik açıdan asıl amacı iletişim güvenliğini sağlamaktır. Günümüzde ağ sistemlerinin çoğu, AAA sistemini kullanmaktadır ancak bu ağların çoğu kamuya açık değildir. Örneğin AAA, birçok çalışanı olan bir şirkette, şirket çalışanlarının birbirleriyle olan iletişiminin güvenliği, gizli iletilerin sadece yetkili kişiler tarafından görülebilmesi gibi amaçlarla kullanılabilmektedir [23]. Bu açıdan bakıldığında, AAA, elektronik imzanın

---

[3] Genel uygulamalara; e-ticaret işlemleri, dosya sunucuları, adres defterleri, elektronik posta, ajandalar ve özel sanal ağlar üzerinde kurulmuş olan güvenli kanallar örnek verilebilir.

[4] İş uygulamalarına; belgelerin dağıtımı ve yayımı, sözleşme yönetimi, elektronik formları yeniden görüntüleme ve zaman yönetimi örnek verilebilir.

kullanılabilmesini sağlayan temel yapıyı oluşturmaktadır. Elektronik imza ile hayata geçirilen işlevlerin birçoğu AAA tarafından sağlanmaktadır.

AAA; elektronik sertifikaların, açık anahtar şifrelemesinin ve SHS'lerin uyumunu sağlayarak geniş bir güvenlik mimarisi oluşturmaktadır. Tipik bir AAA; bünyesinde yer alan kullanıcılara elektronik sertifika verilmesi, sertifikaların yayınlanması, yenilenmesi ve iptal edilmesi ile gerekli teknik desteklerin verilmesi gibi fonksiyonları yerine getirmektedir.

2.2.4.1. Açık anahtar altyapısı bileşenleri

AAA uygulamalarının gerçekleştirilmesi noktasında katkı sağlayan bütün unsurlar, AAA bileşeni olarak değerlendirilmektedir. Söz konusu unsurlar arasında SHS, kayıt kurumu, sertifika dizini, sertifika sahibi ve üçüncü kişi gibi kavramlar yer almaktadır.

2.2.4.1.1. Sertifika hizmet sağlayıcısı

SHS, AAA'nın en önemli bileşenlerinden birisidir. Kohnfelder tarafından 1978 yılında açık anahtar ile herhangi bir elektronik sertifikanın ilişkilendirilmesi teorisi [25] ortaya atıldıktan sonra, güvenilir bir kuruma duyulan ihtiyaç ve kullanılan elektronik sertifikaların geçerliliğinin doğrulanması gerekliliği SHS'nin önemini ortaya çıkarmıştır.

SHS kavramının, "Elektronik Sertifika Hizmet Sağlayıcısı", "Sertifikasyon Kurumu", "Yayınlayıcı Kurum" veya "Sertifika Yayınlayıcı" gibi farklı kullanımları da bulunmaktadır [24].

Kanunda "sertifika hizmet sağlayıcısı" yerine "elektronik sertifika hizmet sağlayıcısı" kavramı kullanılmaktadır. Bu Tez kapsamında, Türkiye'de faaliyet gösteren ve sertifika hizmeti sağlayan kuruluşlar ESHS olarak, diğerleri ise SHS olarak nitelendirilmektedir.

Kanunda ESHS tanımına yer verilmemiş ancak Kanunun 8 inci maddesinde ESHS kavramının çerçevesi *"elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler"* olarak belirlenmiştir.

Elektronik imzanın oluşturulması ve kullanılması süreci doğrultusunda SHS, kayıt, sertifika oluşturma, sertifika dağıtımı, iptal ve iptal durum bilgisi gibi çeşitli hizmetler sunmaktadır [1]. SHS'nin temel görevleri; kullanıcı kimlik bilgilerini doğru tespit etmek, gizli anahtar bilgilerini gizli tutmak, kendi gizli anahtarını saklamak ve korumak için gerekli önlemleri almak ve kimlik ile açık/gizli anahtar çifti arasında ilişki kuran elektronik sertifikaları oluşturmaktır.

SHS, elektronik sertifika verilen kişilerin kimlik bilgilerinin ve sertifika içerisinde yer alacak diğer bilgilerin tam ve doğru bir biçimde tespit edilmesinden ve sertifikalarla açık anahtarların eşleştirilmesinden sorumlu kılınmıştır. Bununla beraber kayıt kurumları da SHS adına bu hizmeti sağlayabilmektedir. Bu çerçevede, kayıt kurumu tarafından yapılan kimlik doğrulamasını müteakip, SHS sertifikayı oluşturmakta ve kendi gizli anahtarıyla imzalamaktadır.

Yukarıda belirtilen hizmetlerin yanında iptal durum bilgisi hizmeti, SHS tarafından gerçekleştirilmesi gereken önemli hizmetler arasında yer almaktadır. İptal durum bilgisi hizmeti, üçüncü kişilere, elektronik sertifikaların geçerlilik durumlarıyla ilgili bilgi sağlayan hizmettir. İptal durum bilgisi hizmeti, sertifika iptallerine ilişkin taleplerin alınmasını, gerekli işlemlerin yapılmasını ve raporlanmasını içermektedir. Bu hizmet sonucu ortaya çıkan sonuçlar iptal durum bilgisi hizmeti vasıtasıyla ilgili taraflara sunulmaktadır. SHS, gerçek zamanlı veya belirli aralıklarla güncellenen iptal durum bilgisi kayıtlarını imzalayarak yayınlamaktadır.

2.2.4.1.2. Kayıt kurumu

Kayıt kurumu, SHS'ye destek vermek ve yardımcı olmak için oluşturulmuş bir alt birimdir. AAA'ya giriş kapısı olarak bilinen bu birim, sertifikalandırma konusunda

işlev görmektedir. Ayrıca kayıt kurumu, kullanıcı ile SHS arasındaki bağlantıyı sağlayacak hizmetleri de verebilmektedir.

Bu birimin en temel görevi, elektronik sertifika içerisine konulacak bilgilerin doğruluğunu kontrol etmek ve onaylamaktır. Bu birimden elde edilen bilgilerle bir sertifika isteği oluşturulmakta ve bu istek SHS'ye iletilmektedir. Bu sayede SHS, güvendiği birimden doğrulanmış bilgileri alarak, kullanıcının güvenli olarak AAA'ya girişini sağlamaktadır [26].

2.2.4.1.3. Sertifika dizini

Sertifika dizini, elektronik sertifikaların geçerlilik durumunu gösteren iptal durum bilgisinin yayınlanması fonksiyonunu yerine getiren bileşendir. Sertifika dizini olarak genellikle ITU-TRec. X.500 (International Telecommunications Union Telecommunications Standardization Sector Recommendation – Uluslararası Telekomünikasyon Birliği Telekomünikasyon Standardizasyon Sektörü Tavsiyesi) veya LDAP (Lightweighted Directory Access Protocol – Hafifletilmiş Dizin Erişim Protokolü) dizin sistemleri kullanılsa da sertifikalara web sunucuları üzerinden erişilmesi mümkün olabilmektedir. Sertifika dizinleri genellikle herkes tarafından erişilebilen yapılardır. Ancak bazı AAA sistemlerinde sınırlı veya ücretli erişim yapılanması da söz konusu olabilmektedir [28].

2.2.4.1.4. Sertifika sahibi

Sertifika sahibi, adına elektronik sertifika düzenlenmiş gerçek kişileri tanımlamaktadır. Literatürde "sertifika sahibi", "imza sahibi" ve "kullanıcı" kavramları aynı anlamda kullanılmaktadır.

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin (Yönetmelik) 15 inci maddesi uyarınca sertifika sahibi bazı hususları yerine getirmek ile yükümlü kılınmıştır. Bu çerçevede sertifika sahibi, açık ve gizli anahtarları ESHS'ye ait olmayan yerlerde ve araçlarla üretmesi durumunda gerekli

güvenliği sağlamalı ve gizli anahtarı kendisi üretmesi durumunda Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Tebliğ) ile belirlenen algoritmaları ve parametreleri kullanmalıdır.

Sertifika sahibinin gizli ve açık anahtarlarını sadece elektronik imza oluşturma ve doğrulama amaçları için kullanması, gizli anahtarını başkalarına kullandırmaması, imza oluşturma aracının veya erişim verisinin[5] kaybolması veya çalınması ile gizli anahtarının gizliliğinden veya güvenliğinden şüphe etmesi durumlarında ESHS'yi derhal bilgilendirmesi ve güvenli elektronik imza oluşturma aracını kullanması gerekmektedir.

2.2.4.1.5. Üçüncü kişi

Üçüncü kişi, atılan elektronik imzaya güvenerek işlem yapan, elektronik sertifikada yer alan bilgileri göz önünde bulundurarak elektronik imzayı doğrulayan kişidir. Yönetmeliğin 16 ncı maddesinde üçüncü kişi; elektronik sertifikanın "nitelikli elektronik sertifika" olup olmadığını, sertifikanın iptal ve geçerlilik durumunu ve sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmek ile yükümlü kılınmıştır.

Üçüncü kişinin elektronik sertifika içerisinde yer alan bilgilerin muteberliğine ne kadar güveneceği birçok faktöre bağlıdır. Bu faktörler arasında; SHS'nin sertifika verirken uyguladığı ilkeler, işletme politikaları ve yöntemleri, uygulanan güvenlik kontrolleri ile sertifika sahibinin ve SHS'nin yükümlülükleri bulunmaktadır [27].

Üçüncü kişi, SHS tarafından verilen elektronik sertifikayı kabul etmesi durumunda bu sertifika içerisinde yer alan bilgilerin doğruluğunu da kabul etmiş sayılır. Elektronik sertifika, güvenilir bir SHS tarafından yayınlanmış olsa da doğrulama yapılırken sertifikanın geçerli olup olmadığı, sertifika durum bilgisi alınarak kontrol

---

[5] Yönetmeliğin 4 üncü maddesinde erişim verisi, güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verileri ifade etmektedir.

edilmelidir. Ayrıca, sertifikada kullanıma dair sınırlamaların yer alması halinde, işlemlerin bu sınırlamalar çerçevesinde yapıldığından emin olunmalıdır [28].

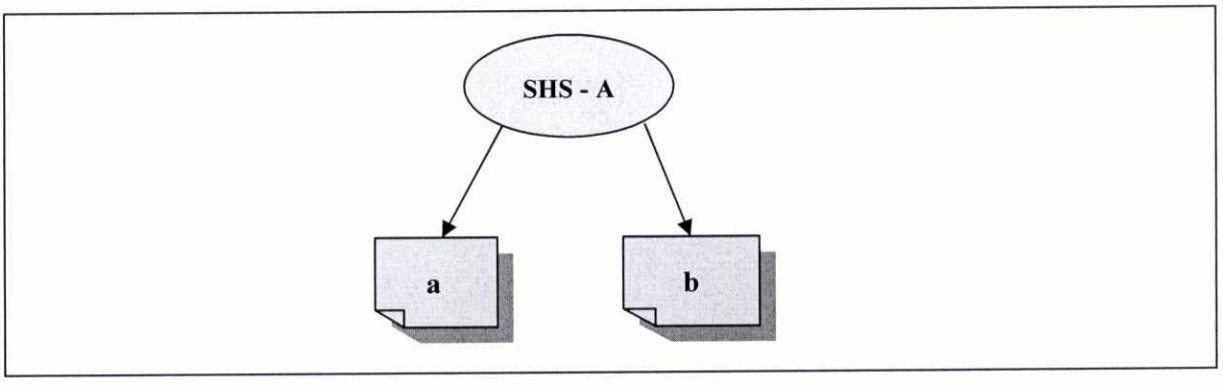
2.2.4.2. Açık anahtar altyapısı modelleri

AAA uygulamaları hayata geçirilirken dört çeşit model dikkate alınmaktadır. Bu modeller; gerek SHS'ler açısından gerekse de kullanıcıların güven duydukları merkez ve SHS'lerin kurdukları güven ilişkisi bakımından birbirinden farklılık göstermektedir [1].

2.2.4.2.1. Tek SHS modeli

Tek SHS modeli, AAA modelleri içindeki en temel ve basit model olarak bilinmektedir. Tek SHS, bu model içindeki tüm kullanıcılar için biricik güven noktasıdır. Bütün sertifikasyon yolları SHS–A'nın kendi elektronik sertifikası ile başlamaktadır. (Şekil 2–6)

Sadece tek bir SHS'nin var olması ve tüm kullanıcılar için sertifikaların hangi uygulamalar için yayınlanacağının bilinmesindeki kolaylık nedeniyle bu modelin uygulanması diğer modellere göre daha basit görülmektedir. Bununla birlikte, bu yapının farklı kullanıcı gruplarını destekleme noktasında yetersiz kaldığı anlaşılmıştır. Kullanıcı grupları arttıkça değişik uygulamaların söz konusu olması nedeniyle tek SHS modelinin uygulanabilirliği zayıflamıştır [29].

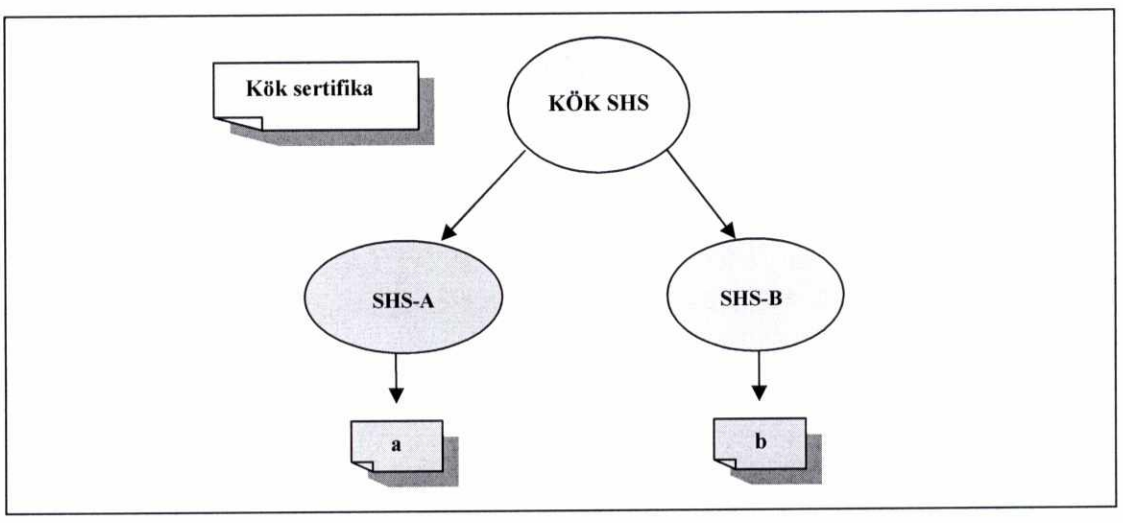


Şekil 2–6: Tek SHS modeli

2.2.4.2.2. Hiyerarşik model

Hiyerarşik üst SHS ilişkilerinin bulunduğu model, hiyerarşik AAA modeli olarak bilinmektedir. Bu modelde tüm kullanıcılar aynı kök SHS'ye güvenmektedir. Yani, hiyerarşik modelde bulunan tüm kullanıcılar için serifikasyon yolu kök SHS'nin elektronik sertifikası ile başlamaktadır. Kök SHS genelde kullanıcılar için değil hiyerarşik olarak altta bulunan SHS'ler için, her alt SHS de kullanıcılar için elektronik sertifika yayınlamaktadır. Hiyerarşik bir modelde güven ilişkisi tek yönlüdür. Diğer bir deyişle, kök SHS alt SHS'ler için elektronik sertifika yayınlamamaktadır. Kök SHS, SHS–A ve SHS–B'nin yayınlayabileceği sertifika türlerine ilişkin koşulları belirlemektedir. (Şekil 2–7)

Basit yapısına ve bağımlı güven ilişkisine bağlı olarak hiyerarşik modelin dört özelliği bulunmaktadır. Kök SHS'nin yeni bir kullanıcı grubunu içine alabilmesi (*ölçeklenebilirlik*) modelin ilk özelliğidir. Sertifikasyon yollarının geliştirilmesi noktasında zorluk yaşanmaması modelin ikinci özelliğidir. Bu özellik bir kullanıcı elektronik sertifikasından güven noktasına uzanan sertifikasyon yolunun basit ve anlaşılabilir olmasını işaret etmektedir. Üçüncü özelliği sertifikasyon yollarının kısa olmasıdır. Modelin son özelliği ise elektronik sertifikaların hangi uygulamalar için kullanıldığının, kullanıcılar tarafından açıkça bilinmesidir [29].

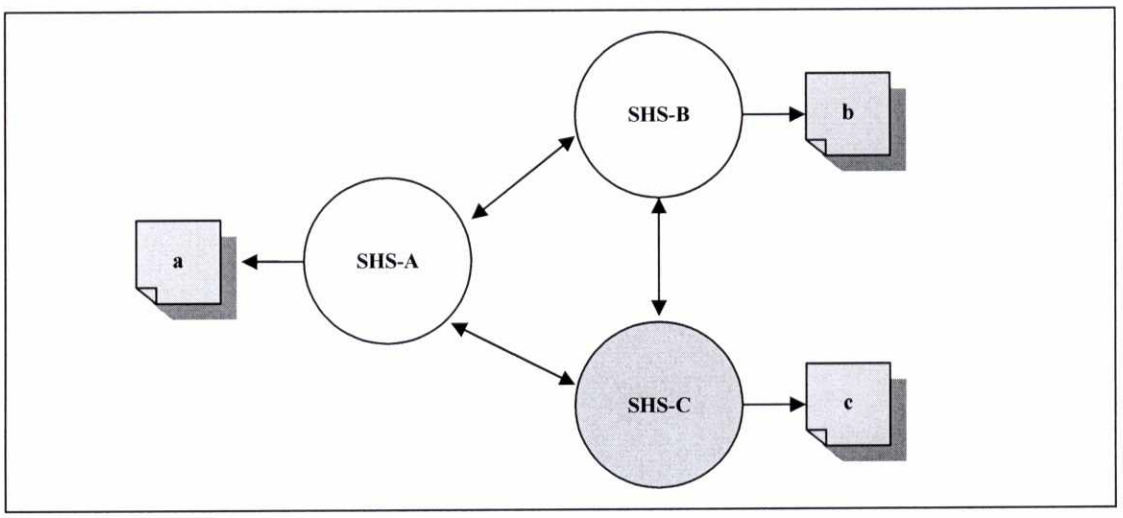


Şekil 2–7: Hiyerarşik model

2.2.4.2.3. Dağıtık model

Hiyerarşik modelin alternatifi, farklı SHS'leri karşılıklı ilişki içinde birbirine bağlayan dağıtık modeldir. SHS'lerin karşılıklı güven ilişkilerinin oluşturulduğu dağıtık AAA modeli Şekil 2–8'de görülmektedir. Dağıtık modelde tüm SHS'ler güven noktası olabilmektedir. SHS'ler birbirleri için elektronik sertifika yayınlamakta, kullanıcılar sertifikalarını yayınlayan SHS'ye güvenmektedir. SHS'ler karşılıklı bir güven ilişkisi içinde bulunduklarından diğer SHS'lerin yayınlayacakları sertifikalara ilişkin koşulları belirleyememektedir.

Dağıtık model, yeni bir kullanıcı grubunu kolaylıkla sürece dâhil edebilmektedir. Modelde yer alan SHS'lerden biri yeni bir kullanıcı grubu ile güven ilişkisini kolaylıkla tesis edebilmektedir. Herhangi bir SHS'nin güvenilirliğini yitirmesi tüm AAA yapısını etkilememektedir. Güvenilirliliğini kaybetmiş SHS'ye elektronik sertifika yayınlayan SHS'ler sertifikaları iptal etmekte ve söz konusu SHS AAA alanının dışına çıkarılmaktadır. Diğer SHS'lere bağlı kullanıcıların hala geçerli bir güven noktası bulunmakta ve bunlar güven ağı içindeki diğer kullanıcılar ile güvenli bir şekilde iletişim kurabilmektedir. En iyi durumda AAA yapısı bir SHS tarafından küçültülmekte, en kötü durumda ise AAA küçük parçalara bölünmektedir. [29].



Şekil 2–8: Dağıtık model

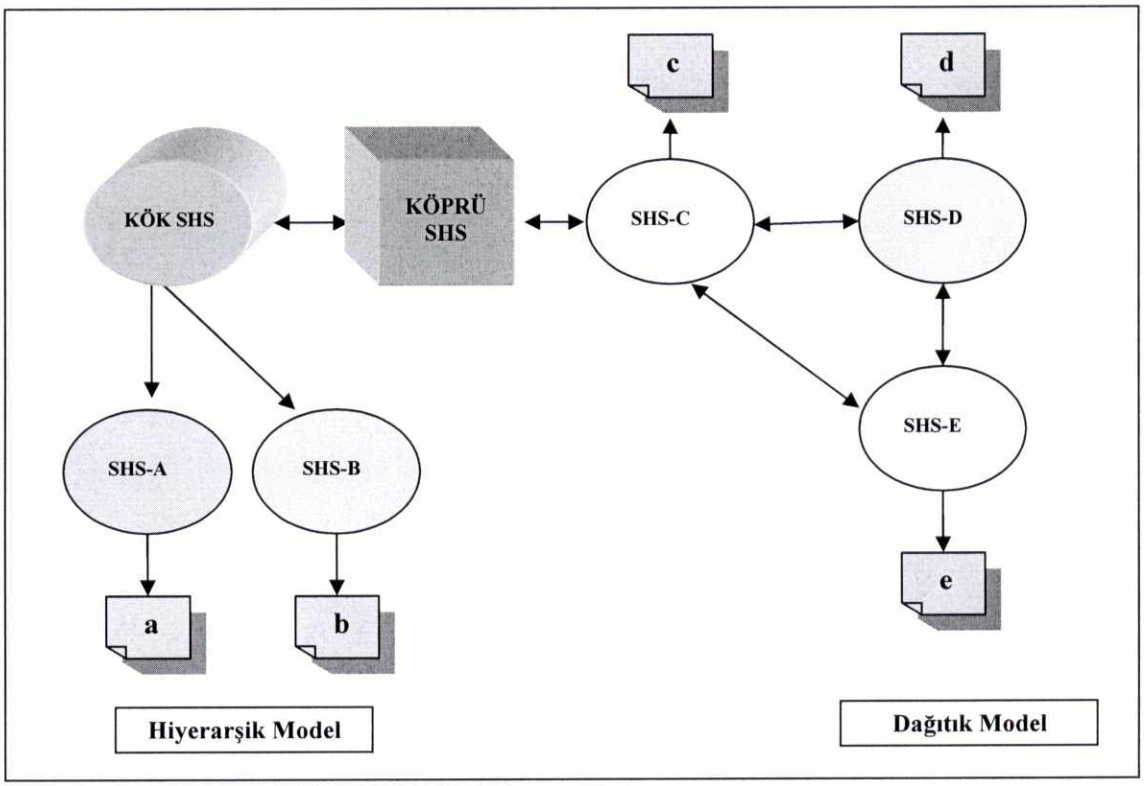
2.2.4.2.4. Köprü modeli

Köprü modelinde farklı sertifikasyon alanlarında bulunan sertifika sahipleri arasında yapılacak elektronik işlemler Köprü SHS üzerinden gerçekleştirilmektedir. Köprü modeli, AAA merkezi olarak nitelenen ve SHS'leri birbirine uyumlu hale getiren bir yöntemdir. Köprü SHS, SHS'lerin altyapıları arasında bağlantı kurmak için hiyerarşik olmayan bir göbek olarak tasarlanmıştır.

Bu yapı bir kök SHS niteliği taşımadığından elektronik sertifika oluşturmamakta, SHS'ler arasında sertifikasyon yolu oluşturmak için karşılıklı güvenlik politikalarının uyumlaştırılması neticesinde güvenli alanları birleştirmektedir. Bu yapıda, sertifika dizini ve sertifika iptal kayıt hizmetleri Köprü SHS tarafından yürütülmektedir. (Şekil 2–9)

Köprü modeli, farklı AAA modellerinin açıklarını kapatmak ve farklı AAA modellerini birbirine bağlamak üzere tasarlanmıştır. Dağıtık AAA modelindeki bir SHS'den farklı olarak Köprü SHS, kullanıcılar için doğrudan elektronik sertifika yayınlamamaktadır. Ayrıca Köprü SHS, hiyerarşik AAA modelindeki kök SHS'nin aksine kullanıcılar için "güven noktası" niteliğini taşımamaktadır. Köprü modeli farklı kullanıcı grupları arasında karşılıklı güven ilişkisi kurmaktadır. Belirli bir güven düzeyinde köprü SHS aracılığı ile farklı kullanıcıların birbiriyle işlem yapmasını teminen bir "güven köprüsünün" tesis edilmesi için söz konusu güven ilişkileri birleştirilmektedir.

Köprü SHS, hiyerarşik ve dağıtık AAA modellerinde yer alan kullanıcılar arasında güven ilişkisi kurmaktadır. Kullanıcı (a), elektronik sertifikasını SHS A'dan almış olup, kök SHS'yi güven noktası olarak tanımaktadır. Kullanıcı (d), sertifikasını SHS D'den almış olup, SHS C'yi güven noktası olarak tanımaktadır. Kullanıcı (a) ve kullanıcı (d), güvenli yollarla birbirleriyle işlem yapabilmek üzere köprü SHS vasıtasıyla güven ilişkisi kurabilmektedir [29].



Şekil 2–9: Köprü modeli

2.2.5. Elektronik imza oluşturma ve doğrulama araçları

Elektronik imza oluşturma aracı, sertifika sahibine ait gizli anahtarın ve elektronik sertifikanın içinde bulunduğu, akıllı kartı ya da benzeri güvenli cihazı, güvenli elektronik imza doğrulama aracı ise, elektronik imzayı doğrulamak amacıyla açık anahtarı kullanan yazılım veya donanım aracını ifade etmektedir [19].

Kanunun 3 üncü maddesinde elektronik imza oluşturma aracı, elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı, imza doğrulama aracı ise elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı olarak tanımlanmıştır.

Kanunun 6 ncı maddesi çerçevesinde güvenli imza oluşturma aracı; ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasına,

üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasına ve gizliliğine, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesine, kullanılamamasına ve elektronik imzanın sahteciliğe karşı korunmasına, imzalanacak verinin imza sahibi dışında değiştirilememesine ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesine ilişkin nitelikleri kapsamaktadır.

Kanunun 7 nci maddesinde imza doğrulama aracı; imzanın doğrulanması için kullanılan verileri ve elektronik sertifikanın doğruluğunu ve geçerliliğini, değiştirmeksizin doğrulama yapan kişiye gösteren, imza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran, imza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren ve imzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan araç olarak tanımlanmıştır.

2.2.6. Zaman damgası

Elektronik imza ile yapılan işlemlerin zaman bilgisinin tespit edilmesi hususu, söz konusu işlemlerin hukuki geçerliliği noktasında büyük önem arz etmektedir. Bu çerçevede, elektronik imza ile imzalanmış dokümanların gönderilmesine veya alınmasına ilişkin zaman bilgisinin ispatı, zaman damgası uygulamasının hayata geçirilmesi ile mümkün olmaktadır. Zaman damgası, elektronik ortamda iletilen mesajlara eklenen ve mesajın yazıldığı zamanı güvenli olarak belgeleyen damgadır.

Kanunun 3 üncü maddesinde zaman damgası *"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.

Zaman damgası hizmetleri; zaman damgası çıkaran teknik bileşen ve zaman damgası çıkarılmasını yöneten, izleyen ve kontrol eden sistem lojistiği olmak üzere iki temel bileşenden oluşmaktadır. Sistem lojistiği güvenilir UTC (Coordinated Universal Time-Koordine Edilmiş Evrensel Zaman) zaman kaynağına doğrudan erişim

sağlamakta ve sistem program bileşenlerinin doğru bir şekilde yönetilmesini garanti altına almaktadır.

Zaman damgası, güvenilir bir kaynaktan zaman bilgisinin alınması ve bu zaman bilgisinin zaman damgasıyla ilişkilendirilecek verinin parmak izi[6] bilgisiyle birleştirilmesi sonucunda oluşturulmaktadır [18].

2.3. Denetim Hakkında Temel Bilgiler

2.3.1. Denetim kavramı

Avrupa'da iktisadi fikir ve uygulamaların geliştiği 16 – 18. yüzyıllarda, uluslararası ticaretin artması sonucu, hesap ve işlemlerin esasa bağlanması gereği denetim kavramını da beraberinde getirmiştir. Bu dönemde hesap ve işlemlerin kontrolünü yapan ve bu kontroller neticesinde görüş beyan eden, Latince "dinleme" anlamına gelen "audit" kelimesinden türetilen auditor (denetim görevlisi) denilen kişiler ortaya çıkmıştır. Modern anlamda denetim kavramı sanayi devrimi sonrasında gelişmiş ve bugünkü niteliğine kavuşmuştur [30].

Denetim kavramıyla ilişkili olarak yakın anlamda kullanılan pek çok kavram bulunmakta olup, kovuşturma, araştırma, soruşturma, inceleme, kontrol, teftiş ve murakabe gibi kavramlar denetim ifadesi yerine kullanılmaktadır [31].

Denetimi tarif etmek amacıyla yapılmış pek çok tanım bulunmaktadır. Türk Dil Kurumu tarafından denetleme kavramı, *"bir görevin yolunda yürütülüp yürütülmediğini anlamak için yapılan araştırma, denetim, bakı, teftiş, murakabe, kontrol"* olarak tanımlanmaktadır [32].

Başka bir tanıma göre denetim; *"yasal, bilimsel, düşünsel yöntemlerle önceden belirlenen standartlardan hareket edilerek işlemlerin ve mevcut uygulamaların bu*

---

[6] Elektronik imzanın oluşturulması ve doğrulanması aşamalarında kullanılan özetleme algoritması, özetleme değerini sayısal olarak temsil etmektedir. Özetleme değerinin sayısal olarak temsil edilmesi "parmak izi" kavramıyla ifade edilmektedir [24].

standartlara uygunluğunun araştırılması, uyumsuzlukların belirlenmesi, giderilmesi ve gelecekte de bu tür risklerin ortaya çıkmaması için yapılan risk ve sistem bazlı proaktif incelemelerdir." [33].

Denetim Kavramları Komitesi[7] tarafından, muhasebe denetimi çerçevesinde, denetim şu şekilde tanımlanmaktadır: *"Denetim; iktisadi faaliyet ve olaylarla ilgili iddiaların önceden saptanmış ölçütlere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla tarafsızca kanıt toplayan ve bu kanıtları değerleyen sistematik bir süreçtir."* [35].

2.3.2. Denetimin unsurları

Denetim, değişik yönlerden çok farklı şekillerde tanımlanabilir. Bununla birlikte esas olan, denetimin temel unsurlarını ve niteliklerini ortaya koymaktır. Önceden belirlenmiş ölçütleri gerekli kılması, süreç niteliğini taşıması, denetlenen birimin standartlara uygunluğunu tespit etmesi, delillerin tarafsızca toplanmasını ve değerlendirilmesini gerektirmesi ve bir sonuca ulaşılmasının gerekmesi denetimin temel unsurları arasında yer almaktadır.

- Denetim için önceden belirlenmiş kıstasların bulunması gereklidir: İncelenmesi istenen hususların doğruluğunun tespiti, ancak daha önceden belirlenmiş kuralların varlığı ile mümkündür. Bu kural veya standartlar arasında; kanunlar, idari düzenleyici işlemler veya düzenleyici kuruluşlar tarafından oluşturulmuş ilke ve standartlar yer almaktadır.

- Denetim aşama aşama incelenmesi gereken bir süreçtir: Denetim faaliyeti, gerekli bilgi ve belgelerin temin edilmesini, bunların işlenmesini ve değerlendirilmesini, değerlendirme sonuçlarına göre bir sonuca ulaşılmasını, ulaşılan görüşün raporlanmasını ve bu raporun ilgililere ulaştırılmasını teminen kaydedilen

---

[7] Denetim Kavramları Komitesi American Accounting Association (Amerikan Muhasebeciler Birliği) bünyesinde faaliyet göstermektedir [34].

aşamaları kapsamaktadır. Bu çerçevede, dinamik ve sistematik bir süreç olan denetim, mantıksal bütünlük içinde birbirini izleyen düzenli aşamalardan oluşmaktadır.

- Denetlenen birimin kurallara veya standartlara uygunluğu denetim ile tespit edilir: Re'sen veya ihbar veya şikâyet nedeniyle yapılan denetimlerle ortaya çıkarılmak istenen husus, denetlenen birimin önceden belirlenmiş kurallara veya standartlara uygunluğunun tespit edilmesi, uygunluk veya varsa uygunsuzluk derecesinin belirlenmesidir.

- Denetim, delillerin hakkaniyet ölçüleri çerçevesinde tarafsızca toplandığı ve değerlendirildiği çalışmalar bütünüdür: Denetim görevlisi önyargısız olmalı, delil ve sonuçları da aynı titizlik ve tarafsızlıkla değerlendirmelidir. Bununla bağlantılı olarak, denetim görevlisi, hakkaniyet kuralları çerçevesinde, ilgili kişi veya kuruluşların aleyhine olan delillerin yanı sıra lehine olan delilleri de takip etmelidir.

- Denetim neticesinde bir sonuca ulaşılmalıdır: Denetim görevlisinin, ileri sürülen iddia ya da incelediği konu ile ilgili olarak yaptığı inceleme çalışmalarına göre bir sonuca ulaşması gerekmektedir. Denetim görevlisi, yaptığı araştırma, inceleme ve ulaştığı bilgi ve belgelere dayanarak bir kanaate ulaşır ve iddia edilen hususları onaylar veya reddeder.

- Denetim sonucu ilgililere rapor halinde sunulur: Raporlama, denetim sürecinin son aşamasıdır. Denetim faaliyetleri neticesinde belirlenen durumların düzenlenecek raporlar ile ilgililere bildirilmesi gerekmektedir. [36].

2.3.3. Denetim türleri

Literatürde denetim türleri ile ilgili birbirinden farklı sınıflandırmalar yapılmaktadır. Denetim türleri ile ilgili olarak en fazla kullanılan sınıflandırma Çizelge 2–2'de yer alan sınıflandırmadır [31].

Çizelge 2–2: Denetim türleri

Amaç Bakımından Denetim Türleri	Mali tabloların denetimi Uygunluk denetimi Faaliyet denetimi Özel amaçlı denetimler
Yapılış Nedeni Bakımından Denetim Türleri	Kanuni denetim İsteğe bağlı denetim
Denetim Görevlisinin Statüsü Bakımından Denetim Türleri	Bağımsız denetim İç denetim

2.3.3.1. Amaç bakımından denetim türleri

2.3.3.1.1. Mali tabloların denetimi

Bir işletmenin sahip veya ortakları, söz konusu işletmenin faaliyet ve sonuçları ile doğrudan ilgilidir. İşletme ile doğrudan ilgili olan sahip veya ortakların yanında, o işletme ile ticari, mali ve ekonomik ilişkiler kuran gerçek kişiler veya kredi, finans ve yatırım kuruluşları ile çeşitli kamu kurum ve kuruluşları işletmenin faaliyet ve sonuçları ile yakından ilgilenmektedir.

Söz konusu hususlarda sağlıklı ve güvenilir bilgi sahibi olmak isteyen kişi, kurum veya kuruluşlar, işletmelerin faaliyet ve sonuçları konusunda bilgi kaynağı niteliğini taşıyan muhasebe kayıt ve belgeleri ile bunlara dayanılarak hazırlanmış mali tabloları dikkate almaktadır. İşletme hakkında bilgi edinmek isteyen gerçek kişi ve kurum veya kuruluşların mali tablolara dayanarak karar almalarındaki en önemli etken, bu bilgilerin mukayese edilebilir nitelikte olmasıdır [37].

Mali tabloların denetiminde, bu tablolardan beklenen amaçların gerçekleşmesini önleyecek aykırılıkların tespiti veya başka bir deyişle, bu tabloların düzenlenme ilkelerine, muhasebe usul ve esaslarına, kanunlara ve önceden saptanmış diğer tüm ölçütlere uygunluk derecesini ölçerek, güvenilirliğinin ortaya konulması amaçlanmaktadır.

Bu denetim, bağımsız denetim görevlileri ve kamu denetim görevlileri tarafından yapılmakta olup, mali tabloların bütünü esas alınarak işletme hakkında genel görüşler oluşturulmakta, aynı zamanda tablolarda yer alacak hatalarla da ilgilenilmektedir [31].

2.3.3.1.2. Uygunluk denetimi

Uygunluk denetimi ile yetkili üst merciler tarafından belirlenmiş kurallara uyulup uyulmadığı hususu araştırılmaktadır [36]. Üst merci, şirket yönetimi olabileceği gibi, herhangi bir kamu kurumu da olabilir. Kamu kurumları veya bağımsız denetim görevlileri tarafından yapılacak uygunluk denetimlerinde amaç, kuruluş veya şirketin birincil veya ikincil mevzuat düzenlemelerine uyup uymadıklarını, bu düzenlemelerle öngörülen yükümlülüklerini yerine getirip getirmediklerini araştırmaktır.

Uygunluk denetimi ile kuruluş veya şirketlerin yasa ve yönetmeliklere uygun hareket edip etmediklerinin belirlenmesi, buna aykırı davranışların en aza indirilmesi hedeflenmektedir [31]. TK tarafından ESHS'lerin denetlenmesi, Maliye Bakanlığı tarafından yürütülen vergi denetimleri ve SPK (Sermaye Piyasası Kurulu) tarafından yapılan denetimler kamu tarafından gerçekleştirilen uygunluk denetimlerine örnek teşkil etmektedir.

2.3.3.1.3. Faaliyet denetimi

Bir işletmenin faaliyetlerinin verimliliğini ve etkinliğini değerlendirmek amacıyla bu faaliyetlerle ilişkili yöntemlerin uygulanışının gözden geçirilmesini kapsayan faaliyet denetiminde, denetim görevlilerinden, tarafsız gözlemlerde bulunmaları ve belirli faaliyetlerin ayrıntılı analizini yapmaları beklenmektedir. Bu çerçevede, işletmenin faaliyet sonuçları önceden belirlenen standartlar ile karşılaştırılmakta ve işletmenin amaç ve hedeflere ne ölçüde ulaştığı ölçülmeye çalışılmaktadır. Faaliyet denetimi, ilgili işletmenin tamamını, bir bölümünü ya da bir şubesini değerlendirmek şeklinde yapılabilmektedir [38].

2.3.3.1.4. Özel amaçlı denetimler

Özel amaçlı denetimler, belli konularda belli bir karar birimine ayrıntılı bilgi sunmak ve önerilerde bulunmak amacıyla ilgili işletmeye ait hesapların, mali tabloların ve bunların dayandığı belgelerin incelenmesi şeklinde gerçekleştirilen denetimlerdir [33]. Yolsuzluk ve ihmallerin araştırılması, mahkemelerce yapılan özel nitelikli incelemeler, vergi incelemeleri, kredi verenlerce yapılan ön incelemeler ile kamu kurum ve kuruluşlarınca yapılan teftiş ve incelemeler özel amaçlı denetimlere örnek olarak verilebilir [31].

2.3.3.2. Yapılış nedeni bakımından denetim türleri

2.3.3.2.1. Kanuni denetim

Kanuni denetimin kaynağını, kanun hükümleri veya kanunun verdiği yetkiye dayanarak hazırlanan ikincil düzenlemeler oluşturmaktadır. Denetimin usul ve esasları, kapsamı, hangi zamanlarda ve ne sıklıkla yapılacağı gibi hususlar kanun veya ikincil düzenlemelerde yer almaktadır. TK, Maliye Bakanlığı ve Hazine Müsteşarlığı gibi kamu kurumları kanuni denetim yapan birimler arasında yer almaktadır [31].

2.3.3.2.2. İsteğe bağlı denetim

İsteğe bağlı denetim, mevzuat açısından bir zorunluluk bulunmamasına karşın, kuruluş veya işletmeler tarafından çeşitli çıkar gruplarının isteği üzerine gerçekleştirilen denetim çalışmasıdır [39].

2.3.3.3. Denetim görevlisinin statüsü bakımından denetim türleri

2.3.3.3.1. Bağımsız denetim

"Bağımsız denetim"; müşterilerine profesyonel denetim hizmeti sunan, tek başına veya bir şirket bünyesinde çalışan ve bağımsız denetim yapabilme konusunda

önceden belirlenmiş şartları karşılayan kimselerce yapılan denetim türü olarak tanımlanabilir. Bağımsız denetim, mali tabloların denetimi, uygunluk denetimi ve/veya faaliyet denetimi türlerinden birini veya birkaçını kapsayacak şekilde yapılabilir [31].

Bağımsız denetim kavramı bazı idari düzenleyici kurumların mevzuatında tanımlanmıştır. EPDK (Enerji Piyasası Düzenleme Kurumu) tarafından hazırlanan Enerji Piyasasında Faaliyet Gösteren Gerçek ve Tüzel Kişilerin Bağımsız Denetim Kuruluşlarınca Denetlenmesi Hakkında Yönetmeliğin [40] 5 inci maddesinde *"Bağımsız Denetim"* kavramı; *"Denetlenene ait faaliyetlerin, uygulamaların, işlem, hesap ve mali tabloların, bağımsız denetim kuruluşunca görevlendirilen denetçiler tarafından bu kuruluşlar adına, genel kabul görmüş muhasebe ilkeleri, Kurulca yürürlüğe konulan hesap ve kayıt düzeni ile mali raporlamaya ilişkin düzenlemeler ve denetlenenin sahip olduğu lisans, sertifika ve yetki belgelerinin ayrılmaz parçasını oluşturan genel ve özel hükümlere uygunluğunun incelenmesi ve bu inceleme sonuçlarına dayanılarak, denetlenen tarafından tutulan hesap, işlem ve kayıtlar ile düzenlenen mali tabloların gerçeği yansıtıp yansıtmadığının tespiti ve rapora bağlanmasıdır."* olarak tanımlanmıştır.

SPK tarafından düzenlenen Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ'de [41] söz konusu kavram; *"İşletmelerin kamuya açıklanacak veya Kurulca istenecek yıllık finansal tablo ve diğer finansal bilgilerinin, finansal raporlama standartlarına uygunluğu ve doğruluğu hususunda, makul güvence sağlayacak yeterli ve uygun bağımsız denetim kanıtlarının elde edilmesi amacıyla bağımsız denetim standartlarında öngörülen gerekli tüm bağımsız denetim tekniklerinin uygulanarak, defter, kayıt ve belgeler üzerinden denetlenmesi ve değerlendirilerek rapora bağlanması"* şeklinde ifade edilmiştir.

2.3.3.3.2. İç denetim

İç denetim, bir kuruluş veya şirketin her biriminde yer alan sistemlerin her aşamasındaki faaliyetlerin yerindeliğini, gerekliliğini ve etkinliğini teminen yapılan

kontrolleri ve bu kontrollerin geliştirilmesine yönelik değerlendirmeleri esas almaktadır [43]. İç denetim kuruluş veya şirket çalışanları tarafından gerçekleştirilmekte, denetime ilişkin raporlama ise kuruluş veya şirket yönetimine yönelik yapılmaktadır.

İç denetim kavramı, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun [42] 63 üncü maddesinde, *"Kamu idaresinin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkililik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız nesnel güvence sağlama ve danışmanlık faaliyetidir."* şeklinde tanımlanmıştır.

İç denetim, denetim alanı itibariyle çok geniş bir kapsama alanını ihtiva etmektedir. Bununla birlikte söz konusu denetim; özü, yapısı, işlevleri ve denetim sonuçları yönlerinden denetlenen birimin üst yönetimiyle sınırlıdır. Denetlenen birimin bizzat kendi personeli olması nedeniyle iç denetim görevlileri, üst yönetimin belirlediği çerçeve içerisinde denetim fonksiyonunu yerine getirmek durumundadırlar. Yapısı gereği iç denetim, örgüt üst yönetiminin kararlarına, planlarına, programlarına, hedef ve stratejileri ile iç ve dış mevzuata uygunluk dışında bir denetim fonksiyonu üstlenememektedir [30].

2.3.4. Genel kabul görmüş denetim standartları

Denetim standartları, denetim organlarına denetim çalışmaları sırasında yol göstermek üzere hazırlanan referans niteliği taşıyan dokümanlardır. Birçok ülkenin kamu denetim organları ve muhasebe kuruluşları denetim standartları yayımlamakla birlikte, denetim organları ve muhasebe kuruluşları tarafından yayımlanan denetim standartları büyük oranda benzerlikler göstermektedir.

Meslek örgütleri tarafından kabul edilmiş olan ve denetim kuruluşları ile denetim görevlilerinin uymak zorunda oldukları standartlara "Genel Kabul Görmüş Denetim Standartları" denilmektedir. İlk defa 1947 yılında AICPA (American Institute of Certified Public Accountants - Amerikan Yeminli Serbest Muhasebeciler Enstitüsü)

tarafından kabul edilmiş olan bu standartlar, bir çok ülkede benimsenmiş ve günümüze kadar çok az değişikliğe uğrayarak gelmiştir.

Genel kabul görmüş denetim standartları denetim faaliyetleri açısından uyulması gereken asgari ve genel nitelikli standartlardır. Her denetim görevlisi genel kabul görmüş denetim standartlarına aykırı olmayan bu denetim standartlarına da uymak zorundadır. Zaman zaman bunlarla ilgili yorumlar ve açıklayıcı alt ilkeler yayınlanmakta, yorumlayıcı ve açıklayıcı nitelikteki ilkelere sadece denetim standartları denilmektedir. Bu nedenle, bunları denetim kurallarının bütünü olarak değerlendirmemek gerekmektedir [31].

Denetim çalışmalarının kalitesinin artırılması, denetim görevlilerinin niteliklerinin, sorumluluklarının ve yapmaları gereken çalışmaların neler olması gerektiğinin belirlenmesi ve denetim görevlilerine yol gösterilmesi gibi hususlar da bu standartların amaçları arasında yer almaktadır. Söz konusu standartlar esas alınarak bütünlüğü, doğruluğu ve tarafsızlığı denetlenip doğrulanmış olan bilgi, tüm karar alıcılar açısından güvenilir bilgi olarak kabul edilmektedir [33].

Denetim işlemlerinin yazılı kurallar haline dönüştürülmesi, denetim faaliyetini kolaylaştırmakta ve denetim görevlisinin hatalı görüş verdiğinin iddia edildiği durumlarda da denetim görevlisinin kendisini savunmasına yardımcı olmaktadır. Bununla birlikte, denetim işlemlerinin ayrıntılı özel kurallar olarak standartlaştırılması yerine davranış ve yargı özgürlüğü tanıyan, izlenmesi gerekli genel davranış kuralları şeklinde geniş kapsamlı tutulmaları daha uygundur [44].

Genel kabul görmüş denetim standartları;

- Genel Standartlar,
- Çalışma Alanı Standartları ve
- Raporlama Standartları

olmak üzere üç gruba ayrılır ve toplam on adettir.

2.3.4.1. Genel standartlar

Genel standartlar; denetim görevlilerinin karakterleri, davranışları ve mesleki düzeyleri ile ilgili esasları içermesi nedeniyle "kişisel standartlar" olarak da adlandırılmaktadır [36]. Bu standartlar denetimin geçerli olabilmesi için denetim görevlilerinde bulunması gerekli olan özellikleri kapsamaktadır. Ayrıca bu ilkeler ile denetim uzmanlığının ve mesleğinin saygınlığının korunması da amaçlanmaktadır.

- Denetim faaliyetinin, yeterli teknik bilgi, deneyim ve uzmanlığa sahip kişi veya kişilerce gerçekleştirilmesi

Denetimle görevlendirilen kişilerin, görevlendirildikleri işleri mevzuat hükümlerine uygun bir şekilde yerine getirebilecek eğitime ve mesleki yeterliliğe sahip olmaları gerekmektedir. Zira yeterli eğitim ve tecrübesi olmayan kişilere denetim görevi verilmesi halinde, denetimden beklenen amaç hâsıl olamamaktadır.

Her ne kadar kişilerin yüksek öğrenim döneminde edindikleri bilgiler denetim çalışmaları için temel teşkil etse de, denetim görevi için istihdam edilen bu kişilerin meslekleri ile ilgili olarak ayrıca bir eğitime tabi tutulmaları büyük önem taşımaktadır. Bununla bağlantılı olarak, ilgililere, bağlı oldukları denetim kurumları tarafından düzenlenen meslek içi eğitim, kurs, seminer gibi programlarla gerekli olan eğitim verilmeye çalışılmalıdır [31].

- Denetim görevlilerinin denetim faaliyetinin her aşamasında bağımsız davranması

Bağımsız davranma, denetim görevlilerinin bağımsız düşünme çerçevesi içinde bulunmaları anlamına gelmektedir. Bağımsızlık, denetim mesleğinin olmazsa olmaz koşuludur. Nitekim denetim görevlisinin bağımsızlığı noktasında bir takım şüphelerin bulunduğu hallerde, denetim sonucunda bildirilen denetim görüşü, bu görüşten faydalanacaklar için anlam taşımayacağı gibi, tarafsızlığın olmadığı bir durumda denetim işlevi de söz konusu olmayacaktır.

Genel kabul görmüş denetim standartlarına göre denetim görevlisinin bağımsızlığına halel getirebilecek hususlar aşağıdaki gibi ifade edilebilir:

- Denetlenen şirketle veya sahipleri ile ortaklık bağının bulunması,
- Denetlenen şirketten maaş, prim veya borç alma gibi nedenlerle maddi menfaat ilişkisinin bulunması,
- Denetlenen şirketin hisse senedi, tahvil ve benzeri araçlarına dolaylı veya doğrudan sahip olunması,
- Denetlenen şirketin ortak veya yöneticileri ile akrabalık bağının bulunması,
- Denetlenen şirketten hediye alınması veya özel bir indirimle pay alınması [45].

Yukarıda belirtilen hususlar denetim görevlisinin bağımsızlığını gölgeleyebilecek haller olup, denetim görevlisinin denetim sırasında söz konusu davranışlardan kaçınması gerekmektedir. Kısaca belirtmek gerekirse denetlenen kişi veya kuruluşlar, denetim görevlisinin bağımsızlığı konusunda şüpheye düşmemelidir.

Denetim görevlisinin tarafsızlığı, bağımsızlığının bir unsurunu teşkil etmektedir. Bu bağlamda, denetim görevlisinin bütünlük içinde hareket etmesi aynı zamanda tarafsızlığının bir parçasıdır. Bütünlükten kasıt, incelenen konunun tüm yönleriyle, tarafların lehine ve aleyhine olan tüm delillerin ortaya konması suretiyle yapılmasıdır. Denetim esnasında belli bir hususun göz ardı edilmesi durumunda denetimin bütünlüğü ortadan kalkacağından bu durum, ortaya çıkacak raporu tarafsızlık açısından olumsuz yönde etkileyecektir [31].

Görevlendirme usulü ve özlük hakları, denetim görevlisinin bağımsızlığını korumak için dikkate alınması gereken diğer önemli unsurlardır [38].

- Denetim faaliyetinin her aşamasında mesleki özen ve titizlik gösterilmesi

Denetim mesleği, denetimin her aşamasında mesleğin gerektirdiği dikkat ve özenin gösterilmesini, denetim standartlarına ve ilgili mevzuat hükümlerine uyulmasını, bilgi, tecrübe ve becerilerin en iyi şekilde kullanılmasını gerektirmektedir.

Denetim sonunda düzenlenen raporlara ilgili kesimler tarafından itibar edilmesi, denetim faaliyetinin titizlikle ve özenle yürütülmesini gerekli kılmaktadır. Denetim görevlisinin mesleki yeterliliğe sahip olmasına ve bağımsız davranmasına karşın, mesleğin gerektirdiği özeni göstermemesi durumunda denetimden beklenen amaçlar hâsıl olmayacaktır. Özensiz şekilde yapılan bir denetim sonucunda ortaya çıkan görüşün fazla bir değeri de olmayacaktır. Bu nedenle, bu görüş nedeniyle karar mercilerinin yanlış kararlar vermesine neden olması durumunda ilgili denetim görevlisinin de sorumluluğu söz konusudur.

Gereken dikkat ve titizliği göstermeyen denetim görevlisi, meslek ahlakına aykırı davranmış olacaktır. Oysa dikkatli ve titiz bir denetim görevlisinin, denetim faaliyetini düzgün bir şekilde planlaması, yeterli sayıda delil toplayarak incelemesi, temiz ve düzgün çalışma kâğıtları hazırlaması, işlemlerle ilgili dürüst bir yargıya ulaşması ve bu yargısını titizlikle düzenleyeceği denetim raporunda ifade etmesi gerekmektedir [36].

2.3.4.2. Çalışma alanı standartları

Çalışma alanı standartları, genel standartlar ile karşılaştırıldığında daha özellikli nitelik taşıyan standartlardır. Sağlıklı bir denetim görüşüne ulaşmak için delil toplama ve delilleri değerlendirme noktalarında denetim görevlisine yol göstermesi, söz konusu standartların en önemli özelliğidir.

Denetim yöntemleri ve öncelikleri gibi konuları kapsayan çalışma alanı standartları; planlama, iç kontrol sisteminin incelenmesi ve denetim delillerinin toplanması standartlarından oluşmaktadır [31].

- Denetim faaliyetinin uygun bir şekilde planlanması

Planlama, denetim faaliyetinin en önemli aşamasını teşkil etmektedir. Sistematik bir süreç olan planlama, işgücünün, zamanın ve kaynakların planlanmasını ihtiva etmektedir.

Denetim faaliyetine ilişkin planlamaya geçmeden önce bir takım bilgilere sahip olunması, diğer bir deyişle, denetlenecek kuruluş veya işletmenin faaliyet alanına, işletmenin kurumsal ve mali yapısına, iş ilişkisi içinde olduğu üçüncü kişilere ve daha önce denetlenecek birim ile ilgili düzenlenmiş denetim raporlarına ilişkin bilgi toplanması gerekmektedir. Bu itibarla, ilgili kuruluş veya işletmenin denetlenmesi için uygun bir denetim planı hazırlama aşamasına geçilmesi ancak söz konusu bilgilerin temin edilmesinden sonra mümkün olmaktadır.

- Denetlenecek işletmenin iç kontrol sisteminin incelenmesi

İç kontrol sistemi, işletmedeki işlemlerin yazılı belgelerde yer aldığı şekliyle yapıldığının önemli bir güvenilirlik göstergesidir. Kurum içinde görülen yanlış uygulamaların ve risklerin azaltılması noktasında etkin bir iç kontrol sistemi büyük bir önem taşımaktadır. Zira iç kontrol sistemi denetim görevlilerinin çalışmalarında dayanak noktası olarak kullanılan oldukça önemli düzenlemelerdir. Denetimin planlanması, yapılacak kontrollerin niteliğinin ve denetim için zaman aralığının tespiti aşamasında, denetlenen işletmenin iç kontrol sistemi hakkında yeterli bilgi edinilmesi gerekmektedir.

- Çeşitli denetim tekniklerinin uygulanarak yeterli delil toplanması

Belge analizi, inceleme, ön araştırma ve soruşturma gibi yöntemler en yaygın denetim teknikleri arasında yer almaktadır. Bu standart marifetiyle, incelenen olayla ilgili bir denetim görüşüne ulaşmadan önce söz konusu denetim teknikleri kullanılarak, bu görüşü destekleyecek uygun, güvenilir ve yeterli delillerin toplanması öngörülmektedir.

Söz konusu standart uyarınca denetim görevlisinin yeterli sayıda ve sonuç elde etmeye yönelik delil toplaması gerekmektedir. Zira delil toplamanın ana nedeni, incelenecek konu hakkında bir denetim görüşüne ulaşmaktır. Delillerin yeterli miktarda olması, incelenen veya denetlenen konuya ilişkin olarak ilgilileri tatmin etmesi ve güvenilir sonuçlar çıkarmaya elverişli olması ile doğru orantılıdır.

Deliller toplanırken dikkat edilmesi gereken faktörler; önemlilik, risk, nitelik, maliyet ve zamanlılık gibi hususlardır [33].

- Önemlilik: Denetlenen işletmede hangi delillerin daha önemli olduğu ve öncelikle elde edilmesi gerektiği hususu, genelde subjektif bir konudur. Hangi işlemin önemli olduğuna, işlemin keyfiyetini ve kemmiyetini inceleyen denetim görevlisi karar verecektir. Ancak diğer işlemlere göre öne çıkan ve denetim görevlisinin kararını etkileyebilecek nitelik ve nicelikte bulunan hususlar, delilin önemliliği noktasında karine teşkil etmektedir. Denetim görevlisi önemlilikle ilgili karar verirken, faaliyetin mali etkilerini özellikle dikkate almalıdır. Ancak, denetim görevlisi, söz konusu faaliyetin mantıksal, psikolojik ve kanuni etkilerini de göz önünde bulundurmak durumundadır.

- Risk: Risk, denetlenen işlemlerde hata veya hile yapılması ihtimalini içermektedir. Denetim görevlisi, riski yüksek olan işlemler ile ilgili daha fazla delil toplamalı, risk ve toplanması gerekli delil arasında orantı kurabilmelidir.

- Nitelik: Delillerin niteliği, delillerin ispat gücünü doğrudan etkilemektedir. Örneğin, imtiyaz sözleşmeleri, noterde yapılmış işlemler ve tapu kayıtları gibi deliller güvenilir kayıtlardır. Buna karşılık üçüncü bir şahsın ifadesine dayanan bilgiler güvenilir kanıtlar değildir. Denetim görevlisi, delil toplarken hatasız delilleri toplamanın yanında, denetim açısından inandırıcı delilleri toplama hususunu da dikkate almalıdır.

- Maliyet: Denetim faaliyeti ile amaçlanan husus, denetlenen işlem veya olayla ilgili inandırıcılığı olan sağlam deliller ile denetim görevlisinin görüş oluşturmasını sağlamaktır. Denetim yapılırken, uygun bir maliyete katlanarak yeterli delil toplanması büyük önem taşımaktadır. Çünkü denetim çalışmaları sırasında, denetim görüşünün yüzde yüz doğruluğunu ortaya koymak amacıyla, yüksek maliyetli bir çabaya girmek doğru bir yaklaşım değildir. Denetim standartları, denetim görevlisinin kaliteli görüşlere sahip olmasını

istemekle birlikte, denetim görevlisinin bu görüşe ulaşırken başvurabileceği çeşitli denetim tekniklerinin en ucuzunu uygulamasını önermektedir [36].

- Zamanlılık: Delillerin zaman açısından denetlenen faaliyet veya işlemlere uygunluğu önemlidir. İncelenen olay ile delillerdeki tarihlerin tutarlı olması önem taşımaktadır. Aksi durumda, delilin denetlenen olayı açıklama veya denetim görüşü oluşturmaya yardımcı olma fonksiyonu ortadan kalkmaktadır.

2.3.4.3. Raporlama standartları

Raporlama standartları, raporlama işlemlerinin önceden belirlenmiş kıstaslara uygun olarak yapılmasını sağlayan standartlardır. Raporlama standartları; genel kabul görmüş muhasebe ilkelerine uygunluk sağlanması, genel kabul görmüş muhasebe standartlarında değişmezlik, mali tablolardaki açıklamaların yeterliliği ve görüş bildirme standartlarından oluşmaktadır [31].

- Genel kabul görmüş muhasebe ilkelerine uygunluk sağlanması

Düzenlenecek denetim raporu, raporun genel kabul görmüş muhasebe ilkelerine uygun olarak hazırlanıp hazırlanmadığını belirtmelidir.

- Genel kabul görmüş muhasebe standartlarında değişmezlik

Düzenlenecek raporda, cari dönem mali tablolarını etkileyen muhasebe yöntem ve teknikleri ile bir önceki dönem mali tablolarını etkileyen muhasebe yöntem ve teknikleri arasında farklılıklar söz konusu ise bunların ayrıntılı bir şekilde açıklanmasına yer verilmelidir.

- Mali tablolardaki açıklamaların yeterliliği

Düzenlenecek raporda aksine bir bilgi yoksa mali tablolarda yer alan açıklayıcı dipnotlardaki bilgiler yeterli kabul edilmektedir.

- Görüş bildirme

Denetim faaliyeti sonucunda düzenlenecek raporda, denetim faaliyeti ile ilgili olarak bir yargıya ulaşılmalı ve bu yargı, mutlaka olumlu görüş, şartlı görüş, görüş bildirmeden kaçınma veya olumsuz görüş belirtmelidir. Bu yargı görüş bildirmekten kaçınma şeklindeyse bu durumun nedenleri ayrıntılı bir şekilde raporda yer almalıdır.

3. DÜNYADA SHS'LERİN DENETİMİNE İLİŞKİN YAKLAŞIMLAR

3.1. Avrupa Birliği Yaklaşımı

Avrupa Birliği'nin elektronik imzaya ilişkin düzenlemeleri 13 Aralık 1999 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlanan 99/93/EC sayılı Elektronik İmza Direktifi [46] ile başlamıştır. Bu Direktif ile Avrupa Birliği üyesi ülkeler için bir çerçeve ortaya konulmuş ve üye ülke düzenlemelerinin 19 Temmuz 2001 tarihine kadar tamamlanması istenmiştir.

Direktifin, elektronik imzanın kullanımını kolaylaştırmak ve yaygınlaştırmak ile hukuken tanınmasına katkıda bulunmak olmak üzere iki amacı bulunmaktadır.

Direktifte, *gelişmiş elektronik imza* ve *elektronik imza* olmak üzere iki farklı imza türü öngörülmüştür. Gelişmiş elektronik imza, güvenli elektronik imza oluşturma aracı tarafından oluşturulan ve nitelikli elektronik sertifika tabanlı bir elektronik imza türüdür. Gelişmiş elektronik imza, hukuken elle atılan imza ile aynı hukuki değerde olan ve delil olarak geçerliliği bulunan elektronik imzadır. Söz konusu hukuki sonuçların hâsıl olması için, nitelikli elektronik sertifikanın Direktif Ek-1'de belirtilen gerekliliklere uygun olması ve SHS'nin Direktif Ek-2'de belirtilen koşulları sağlaması gerekmektedir.

Direktif; elektronik imzanın hukuken tanınmasına, elektronik imza sertifikaları, SHS'ler ve bunların gözetimi ile ilgili esasların belirlenmesine [47] ve elektronik imza ürün ve hizmetlerinde serbest dolaşım ilkesi temel alınarak SHS hizmetlerinin ilgili kuruluşlar için yetkilendirme işlemi gerektirmeden bildirim esasına göre sunulmasına imkân sağlamıştır [48].

Direktif kapsamında, SHS'lerin ilgili mevzuat hükümlerine uygunluğunun tespit edilmesi konusunda denetim, ihtiyari akreditasyon ve sertifikasyon (uygunluk değerlendirmesi) kavramlarına yer verilmiştir.

3.1.1. Denetim

Direktifin 13 sayılı ilkesinde denetimin başlıca amacı, SHS'nin, faaliyetlerini Direktifte belirlenmiş gerekliliklere uygun yürütüp yürütmediğinin kontrol edilmesi olarak tespit edilmiştir. Direktifin 2 nci maddesinde yer alan SHS tanımı çerçevesinde, elektronik sertifika yayınlanmasına ilişkin hizmetlerin yanında elektronik imzaya ilişkin diğer hizmetler de denetim kapsamında bulunmaktadır.

Direktifin SHS'lerin denetimi ile ilgili 3.3 maddesine göre, her üye devlet kendi sınırları içerisinde *kamuya* nitelikli elektronik sertifika hizmeti sağlayan SHS'lerin denetimini yapmak üzere uygun bir yapı kurmak zorundadır. Direktifin 3.3 maddesinde geçen "kamu" kavramı Direktifte tanımlanmamış olup, söz konusu kavram genel anlamda, bütün üye devlet vatandaşlarına aynı şartlarda hizmet sağlanması anlamına gelmektedir. Şirket ağları veya kapalı kullanıcı grupları gibi örnekler kamuya elektronik sertifika hizmetinin sağlanmadığı durumları yansıtmaktadır.

Üye devletler tarafından kurulan denetim yapılarının kapsamı, söz konusu devletlerin sınırları içinde faaliyet gösteren SHS'ler ile sınırlandırılmıştır. Diğer bir deyişle, her bir devlet sadece kendi SHS'lerini denetlemekle yetkili kılınmıştır.

Üye devletlerin, denetim çalışmalarının yürütülmesi noktasında, birbirinden farklı uygulamaları söz konusu olmaktadır. Denetim çalışmaları birçok ülkede, periyodik olarak denetim kurumu tarafından ve/veya denetim kurumu adına bağımsız kurum veya kuruluşlar tarafından yürütülmektedir.[8]

---

[8] FESA (Forum of European Supervisory Authorities for Electronic Signatures - Avrupa Elektronik İmza Denetim Kurumları Forumu), Direktif kapsamında denetim çalışmaları yapmakla sorumlu kurumlara açık olan bir forumdur. FESA'nın amacı söz konusu kurumlar arasında işbirliğini sağlamak ve teknik kuruluşlarla ortak bakış açısı geliştirmektir. FESA'nın üyeleri arasında Direktifin 3.3 maddesi çerçevesinde denetim yapmakla sorumlu olan milli kurumlar, Avrupa Birliği veya Avrupa Ekonomik Alanı kapsamında faaliyet gösteren sertifikasyon kuruluşları veya ihtiyari akreditasyon kuruluşları bulunmaktadır. FESA'ya üye olan kurumlar düzenli olarak yılda üç defa bir araya gelmekte, bu toplantılarda bilgi alışverişi yapılmakta ve denetim kurumları arasında işbirliğine ilişkin konular görüşülmektedir [49].

Avusturya, Belçika, Danimarka, Estonya ve Romanya gibi ülkelerde denetim çalışmaları periyodik olarak yürütülmektedir. Almanya'da ise denetim çalışmaları SHS'nin ilk bildirimde bulunduğu süreçte gerçekleştirilmektedir. Yunanistan, Litvanya ve Bulgaristan gibi ülkelerde ise şikâyet veya ihbar üzerine denetim çalışmaları yapılmaktadır.

Malta mevzuatında, denetim için herhangi bir uygunluk ölçütü belirlenmemiş, Avusturya, İspanya, Polonya ve Slovenya gibi ülkelerde ise düzenlemelere uygunluk denetimi yapılmaktadır. Danimarka, Lüksemburg ve Estonya gibi ülkeler tarafından, denetim kıstaslarını içeren ayrıntılı denetim rehberleri hazırlanmıştır.

Sertifika hizmetlerinin sağlanması faaliyetlerinin yetkilendirme rejimine tabi kılınması veya yetkilendirmeye benzer başka tedbirlerin uygulanması Direktif tarafından kesinlikle yasaklanmıştır. Direktif uyarınca üye ülkelerde faaliyette bulunması için SHS'lerin herhangi bir kuruluştan yetki alması yerine bildirimde bulunmaları hukuken yeterli sayılmıştır. Ancak Almanya gibi bazı ülkelerde, Direktifte bildirim esası öngörülmüş olmasına rağmen, denetim işlevinin yetkilendirme işlevine yakın olduğu görülmektedir [51].

3.1.2. Sertifikasyon (Uygunluk değerlendirmesi)

Bir ürün veya bir hizmeti satın alan kişiler, bu ürün veya hizmetin bazı nitelikleri haiz olmasını beklemekte, bununla birlikte, sunulan ürün veya hizmetin kalitesi hakkında her zaman sağlıklı bir değerlendirme yapamamaktadır. Bu gibi durumlarda sertifikasyon kavramı bu soruna çözüm getirmektedir. Sertifikasyon, bağımsız bir kuruluş tarafından, herhangi bir ürün veya hizmetin belirli nitelikleri taşıdığına ilişkin bir güvenin ilan edilmesi için gerçekleştirilen faaliyetler bütünüdür. Birçok durumda söz konusu nitelikler veya gereklilikler bir standart formatında veya yasal düzenlemelerde veya ilgili taraflarca genel kabul görmüş ilkeler olarak ortaya konulmaktadır. Sertifikalandırılan hususlar arasında ürün, hizmet, idari sistemler (kalite, güvenlik, çevre) ve eğitim gibi konular bulunmaktadır.

İdari sistemlerin sertifikasyonu için en iyi örnek, kurum veya kuruluşların uluslararası ISO 9001 (International Organisation for Standardisation–Uluslararası Standardizasyon Teşkilatı) standardına uygunluğunu sertifikalandıran kalite sistemleridir. Sertifikalandırılan kurum veya kuruluşlara muhatap olan kişiler, bu kurum veya kuruluşların kaliteli bir şekilde hizmet verdiklerinden emin olmaktadır. Aynı durum, bilgi güvenliği konusunda ISO/IEC 27001 standardına uygunluğu sertifikalandırılan kuruluşlar için de geçerlidir. Söz konusu kuruluşlar, sağlanan hizmetlerin kullanıcısı konumunda bulunan kişileri bilgi gizliliği, bütünlüğü ve erişilebilirliği hususlarında tatmin etmek üzere, bilgi saklama, depolama ve taşıma süreçlerini tespit etmekte ve düzenlemektedir. İdari sistemler için verilen bir sertifikanın geçerlilik süresi üç yıl olup, yılda en az bir defa geçici kontroller gerçekleştirilmekte, üç yılın sonunda ise bütüncül bir değerlendirme yapılmaktadır.

SHS'lerin iş süreçleri büyük ölçüde bilgisayar sistemleri, yazılımlar ve iletişim araçları üzerine kurulmuştur. Elektronik sertifika ve zaman damgası gibi hizmetlerin sağlanmasına ilişkin uygulamalar elektronik ortamda gerçekleştirilmekte ve bu uygulamalar için bilgisayar sistemleri kullanılmaktadır. Veri doğrulaması işlemleri harici veritabanları marifetiyle yapılmakta, hizmetlerin sağlanmasına ilişkin bilgiler kullanıcılara elektronik ortamda gönderilmekte ve bu bilgiler kamuya açık veritabanlarında saklanmaktadır. Veri saklamak için kullanılan süreçlerin ve bilgi güvenliği için kullanılan idari sistemlerin uluslararası standartlar ile belirlenmiş kurallara uygun olması gerekmektedir. Söz konusu süreçlerin ve bilgi güvenliği için kullanılan idari sistemlerin sertifikalandırılması durumunda, kullanıcı ve üçüncü kişilerin SHS'nin sağlamış olduğu hizmetlere ilişkin güven sorunu ortadan kalkmış olmaktadır [68].

Direktifin 3.4 maddesinde güvenli elektronik imza oluşturma araçlarının Direktif Ek-3'te belirtilen koşulları karşılayıp karşılamadığını test etmek üzere *"uygunluk değerlendirme kuruluşları"*nın kurulması gerektiği belirtilmektedir. Söz konusu madde kapsamında üye devletler, uygunluk değerlendirmesi yapmak üzere herhangi bir kamu kurumunu veya özel kuruluşu görevlendirmekle yükümlü kılınmıştır.

Avrupa Birliği elektronik imza uygulamalarında çoğu ülkede uygunluk değerlendirme kurumları bulunmamaktadır. Piyasada çok az sayıda ürün olması ve denetim işleminin maliyetinin yüksek olması sebeplerinden ötürü, uygulamada, birçok ülkede imza oluşturma araçlarının uygunluğu, başka ülkelerdeki uygunluk değerlendirme kurumlarının onayı ile tespit edilmektedir. Direktifin söz konusu maddesi, bu uygulamaya izin vermektedir. Buna göre, Direktifte belirtilen koşulları yerine getirmiş bir uygunluk değerlendirme kuruluşu tarafından Direktifte yer alan koşullara göre test edilmiş bir güvenli elektronik imza oluşturma aracının, tüm üye ülkeler tarafından uygun ve geçerli kabul edilmesi gerekmektedir [50].

Birçok ülkede Direktifin 3.4 maddesi hükmü, uygunluk değerlendirmesinin herhangi bir imza oluşturma aracının *güvenli imza oluşturma aracı* olarak tanınması bakımından zorunlu olduğu şeklinde yorumlanmaktadır. İspanya, İngiltere ve Hollanda'da ise uygunluk değerlendirmesi ihtiyari olarak yapılmaktadır [51].

3.1.3. İhtiyari akreditasyon

SHS olan kuruluşların teknik ve idari açıdan yeterliliği ile söz konusu kuruluşların ürün veya hizmetlerini sertifikalandıran sertifikasyon kuruluşlarının gerçekten bağımsız, tarafsız ve profesyonel olup olmadıkları tartışma konusu olmuştur. Bu tartışmaları sona erdirmek için, birçok ülkede devlet tarafından, sertifikasyon işlemlerindeki güvenin teminatı olmak üzere bazı kurum veya kuruluşlar tayin edilmiştir.

1980 yılından bu yana birçok ülkede, gerek SHS'lerin gerekse de sertifikasyon kuruluşlarının güvenilirliğini değerlendirmek üzere akreditasyon kuruluşları kurulmuştur. SHS'lerin veya sertifikasyon kuruluşlarının akredite edilmesiyle birlikte ilgili kuruluşların bağımsızlığı, tarafsızlığı ve profesyonelliği teminat altına alınmış olmaktadır.

Birçok ülkede akreditasyon faaliyetleri, kamu kurumları tarafından yerine getirilmektedir. Değişik Avrupa ülkelerinde kurulmuş olan akreditasyon kuruluşları,

EA (European Co-oparation for Accreditation – Avrupa Akreditasyon İşbirliği) çatısı altında faaliyet göstermektedir. Ayrıca, akreditasyon kuruluşları, sertifikasyon kuruluşları ve sanayi kuruluşlarının uluslararası düzeyde birlikte yer aldığı IAF (International Accreditation Forum – Uluslararası Akreditasyon Forumu) kurulmuştur. EA çatısı altında faaliyet gösteren akreditasyon kuruluşları, aralarında yapmış oldukları sözleşmeler ile birbirlerini karşılıklı olarak tanımakta ve bu çerçevede akreditasyon işlemlerinin güvenilirliğini test edecek yapılar kurmaktadır. [68].

Direktifin 3.2 maddesinde *"Üye devletler sertifika hizmeti sağlama seviyesini ve kalitesini yükseltmek amacıyla ihtiyari akreditasyon yapıları kurabilir. Söz konusu yapılara ilişkin tüm koşullar objektif, şeffaf, oranlı ve ayrım yapmayan nitelikte olmalıdır."* hükmü yer almaktadır. Söz konusu hüküm ile SHS'lerin akreditasyon kuruluşlarına başvurması zorunlu hale getirilmemiş, bu durum tamamen ilgili kuruluşların insiyatifine bırakılmıştır.

İhtiyari akreditasyon, elektronik sertifika sağlama hizmetinin yapılması için, ilgili SHS'nin talebi üzerine, bazı kurum veya kuruluşlar tarafından izin verilmesi prosedürüdür [3].

İhtiyari akreditasyon ile ihtiyari akreditasyon kurumu tarafından belirlenmiş şartların SHS tarafından yerine getirilmesi neticesinde daha kaliteli hizmet sunulması amaçlanmaktadır. Zorunlu akreditasyon kavramı ise denetim kavramına birçok açıdan benzemektedir. Zira denetim sürecinde, zorunlu akreditasyon sürecinde olduğu gibi, denetime tabi kuruluşların denetlenmesi ilgili kuruluşların insiyatifine bırakılmamakta, aksine, bu durumda denetim süreci ilgili kuruluş için zorunlu bir nitelik taşımaktadır.

Zorunlu veya ihtiyari olarak akredite edilen SHS, *akredite olmuş sertifika hizmet sağlayıcısı* vasfını kazanmaktadır. Buna karşın, birçok SHS akredite edildikten sonra bir takım ek yükümlülüklere tabi olmaktadır. Bununla birlikte, akredite edilmiş SHS tarafından yayınlanan elektronik sertifikaların kamu sektöründe kullanımının bazı

ülkelerde zorunlu tutulması nedeniyle akreditasyon kurumları birçok ülkede desteklenmekte ve teşvik edilmektedir [51].

Avrupa Birliği'nde birbirinden farklı akreditasyon uygulamaları bulunmaktadır:

- Birçok ülke mevzuatında ihtiyari akreditasyon kavramına açık bir şekilde yer verilmekle birlikte, Danimarka, Finlandiya, Macaristan ve Polonya gibi ülkelerin mevzuatında ihtiyari akreditasyon konusu düzenlenmemiştir.

- İngiltere ve Hollanda gibi iki istisnanın dışında diğer devletlerde akreditasyon işlemleri kamu kurum veya kuruluşları tarafından yürütülmektedir.

- Avrupa Birliği'nde uygulanan akreditasyon ölçütleri arasında genellikle bir takım farklılıklar bulunmaktadır. Bazı akreditasyon kurumları ulusal mevzuatta belirlenmiş genel kuralları uygularken, diğer kurumlar sadece uluslararası standartları tatbik etmektedir. Örneğin, İtalya'da mevcut SHS'ler İtalyan Elektronik İmza Kanunu çerçevesinde zorunlu olarak akredite edilmektedir. Lüksemburg'da OLAS (Office Luxembourgeois d'Accréditation et de Surveillance – Lüksemburg Akreditasyon Kurumu), SHS'lerin akreditasyonu, denetimi ve denetim görevlilerinin nitelikleri ile ilgili detaylı birçok doküman yayınlamıştır.

- Akreditasyon kurumlarının yapılanması da ülkeden ülkeye farklılık arz etmektedir. Örneğin, Hollanda ve Malta gibi ülkelerde akreditasyon kurumu ile denetim kurumu birbirinden farklı olarak kurulmuş, Almanya'da ise denetim ve akreditasyon işlevleri düzenleyici kurum olan BNetzA (Federal Network Agency for Electricity, Gas, Telecommunications, Postal Service and Railways – Federal Elektrik, Gaz, Telekomünikasyon, Posta Hizmetleri ve Demiryolları Ağı Kurumu)[9] bünyesinde toplanmıştır.

---

[9] RegTP (Regulatory Authority for Telecommunications and Posts – Almanya Telekomünikasyon ve Posta Düzenleyici Kurumu) 13 Temmuz 2005 tarihinde ismini BNetzA olarak değiştirmiştir.

- Birçok akreditasyon kurumunda akreditasyon üç yıl için geçerli olup, bu süre içinde bazı kurumlar düzenli kontrollerini devam ettirmektedir. Avusturya, İtalya, Çek Cumhuriyeti ve Slovenya gibi ülkelerdeki akreditasyon kurumları akreditasyon geçerlilik süresi için herhangi bir sınırlama getirmemiştir. Buradan da anlaşılacağı üzere, bazı ülkelerde SHS'lerin birkaç yılda bir akreditasyonlarını yenilemeleri gerekmekte, bazı ülkelerde ise akredite olmuş SHS'lerin akreditasyon yenilemesine ihtiyaç duyulmamaktadır.

- Bazı ülkelerde SHS'ler, bazı ülkelerde ise sertifikasyon kuruluşları akredite edilmektedir. Örneğin, İsveç ve Hollanda'da sertifikasyon kuruluşları akredite edilmekte, Almanya ve İngiltere'de ise SHS'ler akreditasyon konusu olmaktadır. İsveç'te kurulmuş olan SHS'ler SWEDAC (Swedish Board for Accreditation and Conformity Assessment – İsveç Akreditasyon ve Uygunluk Değerlendirme Kurulu) tarafından akredite edilen bir "sertifikasyon kuruluşu" tarafından değerlendirilmekte ve test edilmektedir. İngiltere'de SHS'leri değerlendirmek üzere sertifikasyon kuruluşu niteliğinde olan tScheme, UKAS (United Kingdom Accreditation Service – Birleşik Krallık Akreditasyon Hizmeti) tarafından akredite edilmektedir [51].

3.2. Ülke Yaklaşımları

3.2.1. Almanya

Bilgi toplumu olma yolunda hızlı adımlarla ilerleyen Almanya, gerek iş hayatında gerekse toplumsal yaşamda internet kullanımının hızla arttığı, buna bağlı olarak, elektronik devlet ve elektronik ticaret uygulamalarında dünyanın önde gelen ülkelerinden birisidir.

Almanya'da nüfusun yüzde 54'ü, şirketlerin ise yüzde 95'i interneti kullanmakta, nüfusun yüzde 22'si ise elektronik ticaret uygulamalarından yararlanmaktadır [52]. Özellikle, 2004 yılından itibaren bankacılık, sağlık ve vergi yönetimi alanlarında elektronik imza kullanımı hızla artmıştır. Yapılan araştırmalar neticesinde 2006 yılı itibariyle yedi milyona yakın kişinin elektronik imza kullanmakta olduğu tespit

edilmiştir. Bu durum, hem elektronik devlet uygulamalarına hem de elektronik ticaret uygulamalarına ilişkin projelerin geliştirilmesine önemli bir zemin hazırlamıştır [53].

3.2.1.1. Elektronik imza mevzuatı

Alman elektronik imza mevzuatı, 1997 yılından itibaren şekillenmeye başlamıştır. Elektronik İmza Kanunu (SigG) [54] 01.08.1997 tarihinde, Elektronik İmza Yönetmeliği (SigV) [55] ise 22.10.1997 tarihinde yürürlüğe girmiştir. 13.12.1999 tarihinde Direktifin uygulanmaya başlanması mevzuatta önemli değişikliklerin yapılmasını gerektirmiştir. Bu nedenle, 16.05.2001 tarihinde Elektronik İmza Kanununda, 16.11.2001 tarihinde ise Elektronik İmza Yönetmeliğinde değişiklikler yapılmıştır. Nihayet, uygulamada yaşanan hukuki sorunların giderilmesini teminen en son 04.01.2005 tarihinde Elektronik İmza Kanununda önemli değişiklikler gerçekleştirilmiştir.[10]

Söz konusu kanunun amacı, elektronik imzanın teknik ve hukuki altyapısını oluşturmaktır. Hukuki olarak zorunlu olmayan hallerde, elektronik imzanın kullanımı ihtiyari nitelik taşımaktadır. Kamudaki uygulamalarda kullanılacak elektronik imza için mevzuat bağlamında ek yükümlülükler getirilebilmektedir.

BNetzA, elektronik imza mevzuatı hükümleri kapsamında, düzenleme ve denetim kurumu olarak görevlendirilmiştir. Elektronik İmza Kanununda genel olarak, SHS'lerin faaliyetleri, ihtiyari akreditasyon, teknik güvenlik ve denetim konularına ilişkin hususlar, Elektronik İmza Yönetmeliğinde ise, söz konusu kanunda yer alan hükümler daha ayrıntılı bir şekilde düzenlenmiştir.

---

[10] Düzenlemelerde değişikliğe gitmenin ana nedenleri arasında, elektronik imza uygulamalarının kolaylaştırılması ve aynı zamanda maliyetlerin azaltılması bulunmaktadır. Önceden bir kişinin elektronik sertifika başvurusu yapabilmesi için bizzat başvuruda bulunması gerektiği halde, yapılan değişiklikler sonucunda SHS'ler, kimlik doğrulaması için kişisel başvuru gerekmeksizin çipli kart oluşturabilmektedir. Bu durum, özellikle mevcut müşteri bilgilerini kullanabilen bankalar için çipli kart oluşturulması sırasında uygulanmaktadır. Ayrıca, çipli kart için internet üzerinden başvuru yapılması da mümkün hale gelmiştir.

3.2.1.2. Elektronik imza altyapı bileşenleri

BNetzA, SHS'lerin bildiriminden ve denetiminden sorumlu olan kurumdur. 25.01.1999 tarihinde milli kök SHS olarak faaliyete geçen BNetzA, SHS'ler ve sertifikasyon kuruluşları için ayrıca akreditasyon kuruluşu olarak da faaliyette bulunmaktadır.

Milli kök SHS olarak teknik faaliyetlerde bulunan BNetzA, akredite edilmiş SHS'ler için elektronik sertifika yayınlamakta ve sertifikaların 7 gün 24 saat doğrulanabildiği bir dizin hizmeti sunmaktadır.

SHS'ler için akreditasyon kuruluşu olarak faaliyet gösteren söz konusu kurum, SHS'ler tarafından idari süreçlerin uygulanması ile kurumsal bilgi ve güvenilirliliğin doğrulanmasına, sertifikalandırılmış güvenlik tedbirlerinin gözden geçirilmesine ve BSI (Bundesamt für Sicherheit in der Informationstechnik – Bilgi Teknolojileri Güvenlik Bürosu) tarafından önerilen uygun algoritmaların ve teknik bileşenlerin Resmi Gazete'de ve internette yayımlanmasına ilişkin hususları takip etmektedir. Elektronik İmza Kanununun 15 inci maddesi uyarınca BNetzA, akreditasyon işlevini yürütürken özel kuruluşlardan da destek alabilmektedir.

Denetim kurumu olarak BNetzA, akredite edilmiş SHS'ler üzerinde düzenli denetim çalışmaları yapmakta ve faaliyetlerin mevzuata uygunluğunu izlemektedir. Denetim işlevinin bir sonucu olarak kurumun önleyici tedbir alma yetkisi de bulunmaktadır. Bu çerçevede, teknik açıdan kullanımı uygun olmayan ürün ve bileşenlerin yasaklanması, elektronik imza ürün ve bileşen sertifikasyonlarının iptal edilmesi, elektronik sertifikaların iptal edilmesi, SHS'lerin faaliyetlerine son verilmesi, faaliyetine son veren SHS'ler ile birlikte bazı faaliyetlerin yürütülmesi gibi çalışmalar da BNetzA'nın yetki kapsamında bulunmaktadır.

Yukarıda belirtilen işlevlerin yanında, BNetzA'nın, güvenlik uygulamaları ve teknik hususlar çerçevesinde sertifikasyon kuruluşlarını yetkilendirmek, bildirim yapan

SHS'lerin bildirim şartlarını yerine getirip getirmediğini incelemek ve bildirim yapan SHS'leri kamuoyuna ilan etmek gibi işlevleri de vardır [56].

BSI, TÜVIT (TÜV Informationstechnik GmbH – TÜV Bilgi Teknolojileri A.Ş.) ve T-Systems (Zertifizierungsstelle der T-Systems – T-Systems Sertifikasyon Merkezi) değerlendirme ve sertifikasyon kuruluşları olarak faaliyet göstermektedir. Söz konusu kuruluşlar, BNetzA tarafından 09.02.1998 tarihinde akredite edilmiştir.

Bu kuruluşlar, elektronik imza ürünlerini ITSEC/CC (Information Technologies Security Evaluation Criteria/Common Criteria – Bilgi Teknolojileri Güvenlik Değerlendirme Kriterleri/Ortak Kriterler) standardına ve elektronik imza mevzuatına uygunluk kapsamında; SUE'nin güvenliğe ilişkin süreçlerini ise elektronik imza mevzuatı çerçevesinde değerlendirmektedir.

Almanya'da yirmidört adet SHS faaliyette bulunmaktadır [57].

3.2.1.3. Sertifika hizmet sağlayıcıları

Almanya'da faaliyet gösteren SHS'ler, akreditasyon ve düzenleme kuruluşu olan BNetzA tarafından akredite edilmektedir. SHS'ler, nitelikli elektronik sertifika ve zaman damgası yayınlayan, sadece nitelikli elektronik sertifika yayınlayan ve sadece zaman damgası hizmeti veren olmak üzere üç grupta toplanmaktadır. Nitelikli elektronik sertifika ve zaman damgası yayınlayan ve sadece nitelikli elektronik sertifika yayınlayan SHS'ler ve akreditasyon tarihleri Çizelge 3–1 ve Çizelge 3–2'de yer almaktadır. 9.11.2001 tarihinde akredite olan AuthentiDate International AG ise sadece zaman damgası hizmeti vermektedir.

Çizelge 3–1: Nitelikli elektronik sertifika ve zaman damgası yayınlayan SHS'ler

Nitelikli Elektronik Sertifika ve Zaman Damgası Yayınlayan SHS'ler	Akreditasyon Tarihi
Produktzentrum TeleSec der Deutschen Telekom AG	22.12.1998
Bundesnotarkammer	14.12.2000
DATEV eG Zertifizierungsstelle	09.03.2001
Steuerberaterkammer Nürnberg	09.03.2001
Hanseatische Steuerberaterkammer Bremen	21.05.2001
Steuerberaterkammer Saarland	21.05.2001
Rechtsanwaltskammer Bamberg	20.08.2001
Rechtsanwaltskammer Koblenz	20.08.2001
Steuerberaterkammer Stuttgart	20.08.2001
Steuerberaterkammer München	20.08.2001
Steuerberaterkammer Berlin	20.08.2001
D-Trust GmbH	08.03.2002
Steuerberaterkammer Niedersachsen	02.09.2002
Hanseatische Rechtsanwaltskammer Hamburg	02.09.2002
Rechtsanwaltskammer München	05.11.2002
Steuerberaterkammer Brandenburg	05.11.2002
Wirtschaftsprüferkammer	21.11.2002
Rechtsanwaltskammer Berlin	21.11.2002
Steuerberaterkammer des Freistaates Sachsen	04.07.2003
Rechtsanwaltskammer Frankfurt am Main	04.07.2003
Rechtsanwaltskammer Nürnberg	09.02.2004
Steuerberaterkammer Nordbaden	23.03.2004
Deutsche Post Com GmbH Geschäftsfeld Signtrust	17.09.2004
TC TrustCenter GmbH	24.05.2006

Çizelge 3–2: Sadece nitelikli elektronik sertifika yayınlayan SHS'ler

Sadece Nitelikli Elektronik Sertifika Yayınlayan SHS'ler	Akreditasyon Tarihi
Patentanwaltskammer	10.03.2004
Steuerberaterkammer Hessen	23.03.2004
Rechtsanwaltskammer Köln	26.10.2004
Rechtsanwaltskammer Düsseldorf	13.09.2005

3.2.1.4. Sertifika hizmet sağlayıcılarının denetimi

Elektronik İmza Kanununun 2 nci maddesinde ihtiyari akreditasyon, elektronik sertifika hizmetinin sağlanması konusunda yetki veren ve belirli hak ve yükümlülükler içeren bir izin düzenleme prosedürü olarak tanımlanmaktadır.

BNetzA, sertifikasyon çalışmaları için gerekli olan güvenilirliğe, bağımsızlığa ve uzmanlığa sahip olduğunu ispat eden kuruluşları, sertifikasyon kuruluşu olarak yetkilendirmiştir. BSI, TÜVIT ve T-Systems sertifikasyon kuruluşları olarak faaliyet göstermektedir. BSI, SHS'lerin uygulaması gereken algoritmaları tespit etmekte, söz konusu algoritmaları BNetzA'ya önermekte ve BNetzA bu algoritma değerlerini Resmi Gazete'de yayımlamaktadır. BSI, TÜVIT ve T-Systems, SHS'lerin güvenlik uygulamalarını[11] uygunluk ve yerindelik bakımından ayrıntılı bir şekilde test etmekte, onaylamakta veya sertifikalandırmaktadır. (Şekil 3–1) Bu durum, SHS'lerin mevzuat ile belirlenmiş gereklilikleri yerine getirdiğine önemli bir karine teşkil etmektedir.

Elektronik İmza Kanununun 15 inci maddesi uyarınca SHS, kanun ile akreditasyon kuruluşu olarak kabul edilen BNetzA'ya akreditasyon başvurusunda bulunabilmektedir. Elektronik İmza Yönetmeliğinin 11 inci maddesi uyarınca akreditasyon başvuruları kâğıt veya elektronik ortamda yapılabilmektedir. SHS'nin akreditasyon başvurusu ihtiyari olup, zorunlu bir nitelik taşımamaktadır. Mevzuat ile belirlenmiş gereklilikleri yerine getirdiğini ispat etmesi halinde SHS akredite edilmektedir.

---

[11] Yönetmeliğin 2 nci maddesinde güvenlik uygulamaları; gerekli tüm teknik, yapısal ve kurumsal güvenlik önlemlerinin tanımını ve bunların uygunluklarını, Kanunun 17 nci maddesi dördüncü fıkrası ikinci bendine göre üretici beyanlarına ya da 17 nci maddesi dördüncü fıkrası birinci bendine ya da 15 inci maddesi yedinci fıkrası birinci bendine göre sertifikasyonlara uygun olarak elektronik imza için kullanılan ürünlerin bir listesini, kuruluşun yapılanması, faaliyetleri ve sertifikasyon çalışmalarına ilişkin değerlendirmeyi, özellikle aciliyet arz eden durumlarda faaliyetleri güvence altına almak ve devam ettirmek için alınan önlem ve tedbirleri, personelin güvenirliliğini değerlendirme ve güvence altına almaya ilişkin usul ve esaslar ile güvenlik risklerinin ölçülmesi ve değerlendirilmesine ilişkin hususları kapsamaktadır.

BNetzA tarafından akredite edilmiş SHS'ye akreditasyon belgesi verilmektedir. Bu belge, teknik ve idari açıdan yapılan kontroller neticesinde, SHS tarafından üretilen elektronik imzanın güvenilirliğinin yeterli ölçüde sağlandığı anlamına gelmektedir. SHS bundan böyle akredite edilmiş SHS olarak kabul edilmekte ve hukuki ve ticari alanlarda güvenlilirliği BNetzA tarafından kanıtlanmış olarak faaliyet göstermektedir.

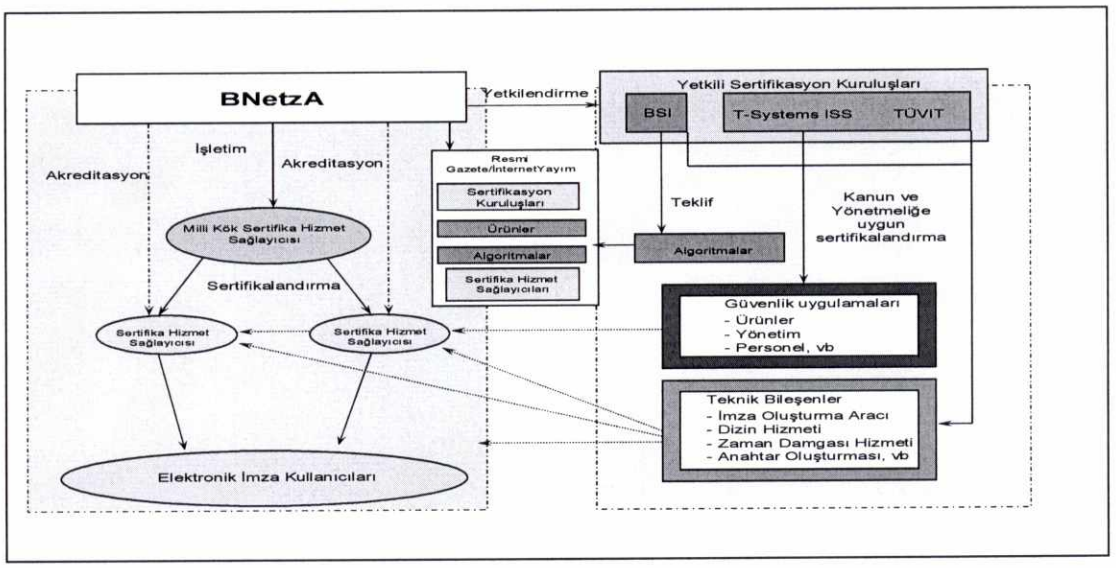
Akredite edilmiş SHS; sertifika hizmeti sağlama faaliyetlerinde sadece sertifikasyon kuruluşları tarafından onaylanmış veya sertifikalandırılmış ürünleri kullanmak ve sadece sertifikasyon kuruluşları tarafından onaylanmış veya sertifikalandırılmış güvenli imza oluşturma araçlarını kullanan kişiler için nitelikli sertifika yayınlamak zorundadır. Söz konusu gerekliliklerin faaliyetlerin devamı sırasında yerine getirilmediğinin tespit edilmesi halinde akreditasyon işlemi iptal edilmektedir.

BNetzA'nın denetim yetkisi, SHS'lerin faaliyete geçmesi ile birlikte başlamaktadır. SHS'lerin elektronik imza mevzuatına uygunluğunun denetimi BNetzA tarafından gerçekleştirilmektedir. Bununla birlikte BNetzA, denetim görevini ifa ederken bağımsız kuruluşlardan da yararlanabilmektedir.

BNetzA, SHS'lerin elektronik imza mevzuatı hükümlerine uygun hareket etmelerini sağlayacak tedbirler almaktadır. Bu çerçevede, SHS'nin bu faaliyetlerin icrası için gerekli olan güvenilirlik seviyesine sahip olmadığını, gerekli uzman kişilere sahip olduğunu ispat edemediğini, gerekli teminata sahip olmadığını, elektronik imza için uygun olmayan ürünleri kullandığını veya faaliyetlerini icra edebilmesi için aranan diğer şartları yerine getirmediğini tespit etmesi durumunda, SHS'nin faaliyetlerine geçici olarak, kısmen veya tamamen son verebilmektedir.

BNetzA, nitelikli elektronik sertifikanın sahte olduğunu veya sahteciliklere karşı yeterli ölçüde güvenli olmadığını veya güvenli imza oluşturma araçlarının elektronik imzada fark edilmeyen sahteciliklere veya bununla imzalanan verilerde fark edilmeyen hilelere yol açan bazı güvenlik hatalarına neden olduğunu tespit etmesi

halinde, nitelikli elektronik sertifikanın iptal edilmesini talep edebilmektedir [54], [55].



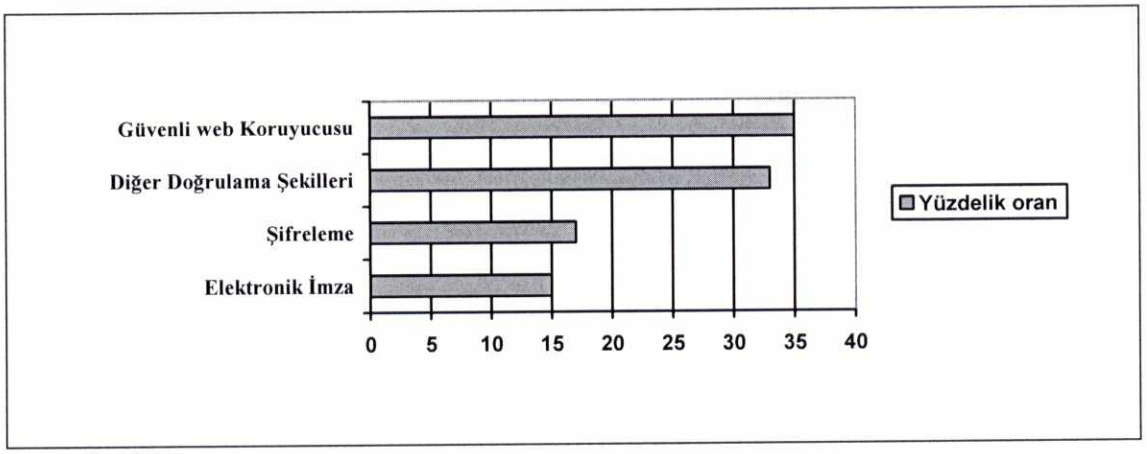
Kaynak [58]

Şekil 3–1: SHS'lerin denetim yapısı (Almanya)

3.2.2. Hollanda

Bilgi teknolojileri alanında üst sınıf ülkelerden birisi olan Hollanda, bilgi ve iletişim teknolojilerinde yaşanan gelişmeleri destekleme hususunda önemli adımlar atmıştır [59]. Bu adımların sonucu olarak, Hollanda, elektronik devlet hizmetlerinin kalitesi ve kullanımı açısından Avrupa ülkeleri içinde Norveç ve İngiltere'den sonra üçüncü sırada yer almaktadır [60].

Gerek elektronik devlet gerekse de elektronik ticaret uygulamalarının yaygınlığı bakımından önemli bir unsur olan elektronik imzanın Hollanda'da kullanımı gerçek ve tüzel kişiler arasında hızla artmaktadır. Hollanda'da faaliyet gösteren şirketlerin yüzde 15'i, bilgi ve iletişim teknolojileri uygulamalarında güvenliği sağlamak için elektronik imzayı tercih etmektedir. (Şekil 3–2) Hollanda'da internet kullanıcılarının ise yüzde 62'si elektronik imzayı kullanmaktadır [61].



Kaynak [61]

Şekil 3–2: Elektronik imza kullanımı (Hollanda)

3.2.2.1. Elektronik imza mevzuatı

Direktif çerçevesinde hazırlanan Elektronik İmza Kanunu [62] 21.05.2003 tarihinde yürürlüğe girmiştir. Söz konusu kanun ile elektronik imza kullanımının yaygınlaştırılması ve elektronik imzanın elle atılan imza ile aynı hukuki geçerliliğe sahip olması amaçlanmaktadır. Elektronik İmza Kanunu, elle atılan imzaya hukuken denk olan ve belirli güvenilirlik koşullarını karşılayan elektronik imza kavramını öngörmüştür.

Elektronik sertifika hizmetlerini sağlamak üzere faaliyette bulunan SHS'ler için ayrıca *"güvenilir üçüncü kişi"* ifadesi de kullanılmaktadır. Elektronik İmza Kanunu kapsamında yapılan ikincil düzenlemelerde, elektronik imzanın doğurduğu hukuki sonuçlar ve SHS'lere ilişkin hükümler yer almaktadır [63].

3.2.2.2. Elektronik imza altyapı bileşenleri

PKIoverheid (Hollanda Devlet Açık Anahtar Altyapısı), kamu kurumları arasında güvenli elektronik iletişimin sağlanması amacıyla kurulan altyapıyı ifade etmekte olup, Hollanda İçişleri Bakanlığı'na bağlı olarak faaliyet göstermektedir. PKIoverheid altyapısında bir kök SHS ve üç SHS bulunmaktadır. Kamu

görevlilerinin elektronik sertifikaları, kök SHS olan PKIoverheid'ın altında bulunan SHS'ler tarafından verilmektedir. SHS'lerin PKIoverheid'ın kapsamında hizmet verebilmesi için ilgili mevzuat hükümlerine uygun olarak faaliyete geçmeleri gerekmektedir [64].

Düzenleme ve denetleme kurumu olan OPTA (Independent Post and Telecommunications Authority – Bağımsız Posta ve Telekomünikasyon Kurumu), Telekomünikasyon Kanunu çerçevesinde, elektronik sertifika hizmetlerini sağlayan SHS'ler ile ilgili düzenleme ve denetleme yapmaya yetkili kılınmıştır. OPTA, Hollanda'da faaliyet gösteren ve nitelikli elektronik sertifika yayınlayan tüm SHS'leri listelemektedir [65]. Söz konusu kanun kapsamında, SHS'lerin OPTA'ya bildirimde bulunması zorunlu kılınmıştır [66].

RvA (Raad Voor Accreditatie – Hollanda Akreditasyon Konseyi), Hollanda'da kamu alanında faaliyet gösteren tek akreditasyon kuruluşudur [67]. SHS'lerin güvenlik süreçlerini ve kurumsal güvenilirliğini sertifikalandıran sertifikasyon kuruluşlarının, söz konusu sertifikasyon işlemlerinin güvenilirliği için yetkili bir akreditasyon kuruluşu tarafından akredite edilmesi gerekmektedir [68]. Bu çerçevede, sertifikasyon kuruluşlarının akreditasyonu ihtiyari olmaktan çok, zorunlu bir nitelik arz etmektedir.

Son yıllarda kurulan TTP. NL (Trusted Third Party of the Netherlands – Hollanda Güvenilir Üçüncü Taraf) ihtiyari akreditasyon kuruluşu olarak faaliyet göstermektedir. Bu kuruluş, talep eden SHS'leri ETSI TS 101 456 standardına uygunluk çerçevesinde akredite etmektedir. TTP. NL, Ekonomik İşler Bakanlığı tarafından desteklenmekte, ECP. NL (Electronic Commerce Platform of the Netherlands – Hollanda Elektronik Ticaret Platformu)'nin yönetimi altında faaliyet göstermektedir [69].

Hollanda'da KPMG (Klynveld Peat Marwick Goerdeler) ve PricewaterhouseCoopers Certification isimli iki adet sertifikasyon kuruluşu bulunmaktadır. Denetim ve danışmanlık hizmetleri veren KPMG ve PricewaterhouseCoopers Certification ETSI

TS 101 456 (European Telecommunications Standards Institute Technical Specification – Avrupa Telekomünikasyon Standartları Enstitüsü Teknik Özellikleri) standardı çerçevesinde SHS'lerin faaliyetlerine yönelik olarak sertifikasyon hizmeti vermektedir [70].

Getronics PinkRoccade, DigiNotar ve CIBG (Central Information Point-Health Care Professionals – Merkezi Bilgi Noktası-Sağlık Bakım Profesyonelleri) yetkili SHS'ler olarak faaliyet göstermektedir [71].

3.2.2.3. Sertifika hizmet sağlayıcıları

2003 yılında faaliyete geçen Getronics PinkRoccade; elektronik ortamda güvenliğin ve çevrimiçi iletişimin gizliliğinin sağlanmasının yanında, elektronik imzaya ilişkin hizmetlerin sağlanması noktasında da faaliyette bulunmaktadır. *"PinkRoccade Trusted Services"* Getronics PinkRoccade'nin operasyon merkezi niteliğini taşımakta olup, AAA ürünlerini ve hizmetlerini VeriSign ile bağlantılı olarak sunmaktadır. PinkRoccade Trusted Services, SHS olarak elektronik sertifika oluşturma ve yayınlama gibi hizmetleri vermektedir. PinkRoccade Trusted Services, VeriSign güven ağının önemli bir bileşenini oluşturmaktadır [72].

1997 yılında faaliyete geçen DigiNotar, SHS olarak, şirketlere internet üzerinde güvenli bir şekilde kimlik doğrulaması hizmetini vermektedir. DigiNotar, bilgi teknolojileri alanında noterler arasında tesis edilen işbirliğini temsil etmektedir. DigiNotar farklı türlerde elektronik sertifika yayınlayabilmektedir [73]. DigiNotar yaklaşık elli noter ile çalışmakta olup, noterlerin internet ortamında yapabilecekleri işlemler üzerinde çeşitli çalışmalar yapmıştır. DigiNotar 2005 yılı itibariyle birkaç bin adet nitelikli elektronik sertifika ve yüzbin adet düzeyinde elektronik sertifika yayınlamıştır [74].

2005 yılında faaliyete geçen CIBG, Hollanda Sağlık Bakanlığı'na bağlı olarak faaliyet gösteren SHS'dir. CIBG, sağlık hizmetlerinde kimlik doğrulama yapısını kurmuştur [75]. Sağlık hizmetlerini sağlayan birimler, UZI (Unieke Zorgverleners

Identificatie – Tekil Kimlik Doğrulama) kartlarını kullanarak kimlik doğrulaması yapabilmektedir [76].

3.2.2.4. Sertifika hizmet sağlayıcılarının denetimi

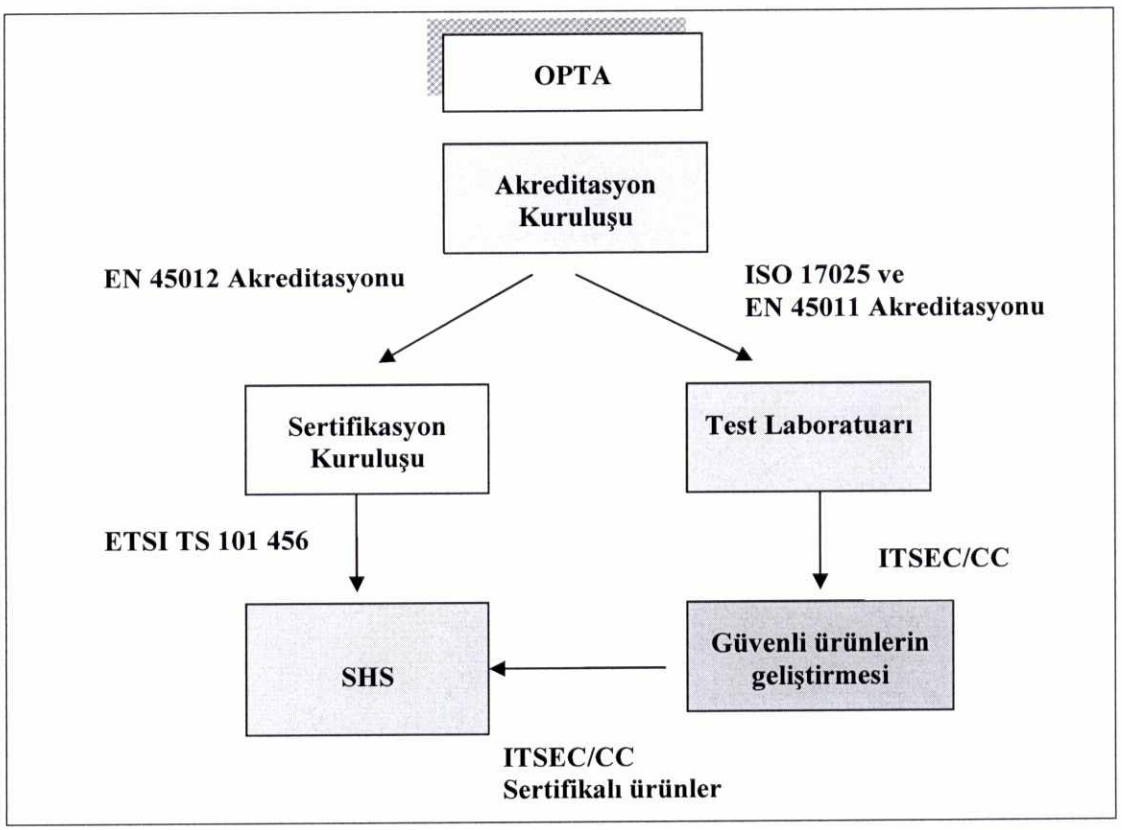
Elektronik imza mevzuatına göre OPTA, bildirimi müteakip, SHS'lerin mevzuatta belirlenmiş düzenlemelere uyup uymadıklarını denetlemekte ancak klasik anlamda denetim yapmamaktadır [65].

Sertifikasyon süreci, sertifikasyon kuruluşu tarafından aşama aşama gerçekleştirilmektedir. Uygunluk sertifikası için başvuruda bulunan SHS, sertifika ilkelerinde belirlenmiş gereklilikler dikkate alınarak sertifikalandırılmaktadır.

SHS ilk aşamada; sertifika ilkeleri dokümanını, nitelikli elektronik sertifikalara ilişkin hususları belirten sertifika uygulama esasları dokümanını, anahtar yönetim ve sertifika yönetim süreçlerini düzenlemektedir. İkinci aşamada; SHS'nin uyması gereken gereklilikleri belirleyen yönetim sistemi oluşturulmakta ve ilgili gereklilikler uygulanmaktadır. Üçüncü aşamada; bilgi güvenliğine ilişkin risk değerlendirmesi yapılmakta, yapılan değerlendirmenin sonucunda bir güvenlik politikası dokümanı hazırlanmakta, bu dokümanın uygulanması için alınması gereken tedbirler tanımlanmakta, bilgi güvenliği için yönetim sistemi oluşturulmakta ve uygulanmaktadır. Dördüncü aşamada ise; SHS, RvA tarafından akredite edilmiş bir sertifikasyon kuruluşuna uygunluk sertifikası başvurusunda bulunmakta ve sertifikasyon kuruluşu SHS hakkında inceleme başlatmaktadır [68].

Akreditasyon kuruluşu, sertifikasyon kuruluşunu EN 45012 (Kalite Sistem Belgelendirmesi Yapan Belgelendirme Kuruluşları İçin Genel Kriterler) standardına, sertifikasyon kuruluşuna bağlı test laboratuarını ISO 17025 (Deney ve Kalibrasyon Laboratuarlarının Yeterliliği İçin Genel Şartlar) ve EN 45011 (Ürün Belgelendirmesi Yapan Belgelendirme Kuruluşları İçin Genel Kriterler) standartlarına göre akredite etmektedir. Söz konusu test laboratuarında güvenli bilgi teknolojileri ürünleri test edilmekte, değerlendirilmekte ve sertifikalandırılmaktadır.

Söz konusu ürünler ITSEC/CC standardı dikkate alınarak geliştirilmekte, böylece, SHS ITSEC/CC sertifikalı ürünleri kullanmaktadır. Sertifikasyon kuruluşu, sertifika ilkelerinde belirtilen gerekliliklere ve ETSI TS 101 456 standardına uygunluğu bakımından SHS'yi sertifikalandırmakta ve konuya ilişkin rapor hazırlamaktadır. Sertifikasyon kuruluşu tarafından hazırlanan raporlar OPTA'ya gönderilmekte, bu raporlar çerçevesinde SHS'nin söz konusu düzenlemelerde belirlenen yükümlülükleri yerine getirmediğini tespit etmesi durumunda OPTA'nın, idari yaptırım ve tedbir alma yetkisi bulunmaktadır [68]. (Şekil 3–3)



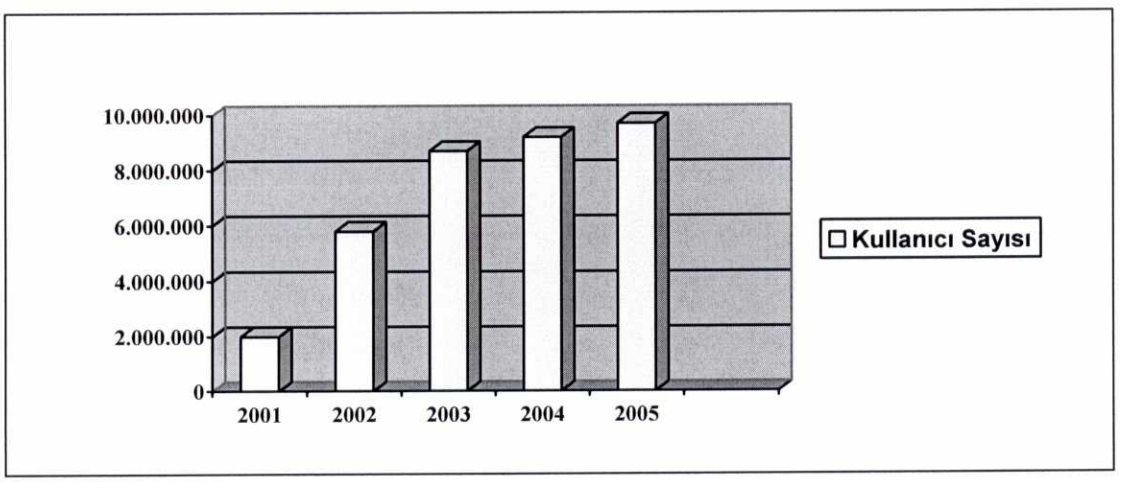
Kaynak [68]

Şekil 3–3: SHS'lerin denetimi (Hollanda)

3.2.3. Güney Kore Cumhuriyeti

Güney Kore, bilişim alanında dünyanın önde gelen ve özellikle elektronik devlet uygulamaları ile dikkatleri çeken bir ülkedir. Gerek bilişim alanında gerekse de elektronik devlet uygulamalarında ortaya çıkan başarının altında yatan en önemli faktörlerin başında bilgisayar okuryazarlığına verilen büyük önem gelmektedir. Bu çerçevede özellikle eğitim, araştırma ve geliştirme alanlarında yapılan yatırımların sonucunda Güney Kore'nin genişbant internet aboneliği alanında yüzde 24,9 ile dünya birincisi ve internet kullanımında dünya üçüncüsü olduğu görülmektedir. 2005 yılı itibariyle nüfusun yaklaşık 48 milyon olduğu ülkede, kullanılan bilgisayar sayısı 30 milyona yaklaşmış bulunmaktadır [77].

Yukarıda belirtilen istatistiksel değerler, Güney Kore'nin bilişim teknolojilerindeki gelişimini işaret etmektedir. Bu durumun doğal sonucu olarak ülkede yaygınlaşan elektronik devlet ve elektronik ticaret uygulamalarının temel altyapısını teşkil eden elektronik imzanın kullanımı her geçen yıl artmaktadır. Güney Kore Bilgi ve İletişim Bakanlığı verilerine göre 2001 yılı itibariyle iki milyon kişi, 2005 yılı itibariyle on milyona yakın kişi için elektronik imza kullanmak üzere elektronik sertifika üretilmiştir [79]. (Şekil 3–4) Elektronik imzanın kullanımında yaşanan artışla paralel olarak, SHS'lerin önemi giderek artmaktadır.



Şekil 3–4: Elektronik imza kullanımı (G.Kore)

3.2.3.1. Elektronik imza mevzuatı

Elektronik Ticaret Kanunu ve Elektronik İmza Kanunu, elektronik ortam güvenliği ve sertifikasyon konularına ilişkin olarak düzenlenmiştir. 1999 yılında yürürlüğe giren Elektronik Ticaret Kanununda, elektronik dokümanların kâğıt ortamda hazırlanan dokümanlarla aynı hukuki geçerliliğe sahip olduğu belirtilmiştir. Söz konusu kanun ile elektronik ticaret uygulamalarının geliştirilmesi, tüketicilerin korunması ve elektronik ticareti destekleyecek politikaların uygulanması amaçlanmıştır [78].

Direktif ve UNCITRAL (United Nations Commission on International Trade Law – Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)'den esinlenerek hazırlanan Kore Elektronik İmza Kanunu 1999 yılında yürürlüğe girmiş, 2001 yılında ise revize edilmiştir [79]. Söz konusu kanunda, SHS'lerin yetkilendirilmesine ilişkin hususlar ile elektronik dokümanların güvenliğinin ve güvenilirliğinin sağlanmasına dair hükümler yer almaktadır.

3.2.3.2. Elektronik imza altyapı bileşenleri

Güney Kore'de elektronik imza hizmetleri, Bilgi ve İletişim Bakanlığının yetkilendirdiği SHS'ler tarafından yerine getirilmektedir. Ayrıca ilgili Bakanlık, sertifikasyon hizmetlerinin yürütülmesine ilişkin hususlarda politika belirlemek, bunların uygulanmasını sağlamak ve yabancı devletler ile uyumlu çalışabilirlik anlaşmaları yapmakla da yetkilidir [85].

Bilgi ve İletişim Bakanlığı, sertifikasyon uygulamalarını[12] güvenilir bir şekilde yürüteceğine güvenilen kurum veya kuruluşları mevzuat çerçevesinde SHS olarak akredite etmektedir [80]. Kamu kurum veya kuruluşları ile tüzel kişiler SHS olarak yetkilendirilecek kuruluşlar arasında yer almaktadır.

---

[12] Kanuna göre sertifikasyon uygulamaları, sertifikaların yayınlanmasını ve sertifikalara ilişkin kayıtların saklanmasını içeren hizmetleri kapsamaktadır.

KISA (Korea Information Security Agency – Kore Bilgi Güvenliği Dairesi Başkanlığı), Bilgi Kullanımını Destekleme ve İletişim Ağını ve Veri Koruma Kanununun 52 nci maddesi uyarınca 1996 yılında kurulmuştur. KISA, Güney Kore'de kök SHS konumunda bulunmaktadır [81]. KISA, yabancı ülkelerde faaliyet gösteren kök SHS'ler ile uyumlu çalışabilirlik anlaşmaları yapmak, yetkilendirilmiş SHS'lerin elektronik sertifikalarını doğrulamak, SHS'leri denetlemek ve AAA uygulamalarının gelişimine katkıda bulunmak hususlarında yetkili kılınmıştır. Bilgi güvenliği için gerekli olan teknolojik altyapı üzerine araştırma ve geliştirme çalışmalarını yürütmek, Kore Elektronik İmza Kanununun [82] 8 inci ve 25 inci maddelerinin amir hükümleri çerçevesinde SHS'lerin açık anahtarlarını doğrulamak, sertifikasyon ile ilgili diğer işleri yürütmenin yanında elektronik imza teknolojisini yaymak ve geliştirmek suretiyle elektronik imzanın güvenli bir şekilde kullanılması için uygun bir ortamı oluşturmak ve SHS'leri etkin bir şekilde yönlendirmek KISA'nın en önemli görevleri arasında bulunmaktadır [81].

KISA'nın himayesinde kurulmuş olan KCAC (Korea Certification Authority Central – Kore Merkezi Sertifikasyon Kurumu), elektronik imzanın kullanımını etkin hale getirmek için birçok faaliyet gerçekleştirmektedir. KCAC'nin; sertifikasyon yönetim sistemini kurmak ve işletmek, SHS'ler için sertifikasyon hizmetlerini sağlamak ve yabancı SHS'ler arasında karşılıklı çapraz tanıma[13] işlemini gerçekleştirmek gibi işlevleri bulunmaktadır.

Bilgi ve İletişim Bakanlığı tarafından yetkilendirilen SHS'ler ise sertifika talebinde bulunan kişilerin kimlik doğrulamasını müteakiben elektronik sertifika oluşturmak ve yayınlamak, yayınlanmış sertifikaların yönetimini sağlamak ve kullanıcı sertifikalarını doğrulamak ile sorumlu kılınmıştır [81],[83].

[13] Çapraz tanıma modeli iki tek yanlı güven ilişkisinin birleştirilmesi olarak tarif edilmektedir. Çapraz tanıma herhangi bir AAA alanındaki sertifika sahibinin başka bir AAA alanında doğrulama yapabilmesi için uygulanan uyumlu çalışabilirlik modelidir.

3.2.3.3. Sertifika hizmet sağlayıcıları

Ülke çapında uygulanan elektronik ihale, elektronik eğitim ve elektronik vatandaş gibi ağ hizmetlerinin güvenliğinin sağlanması için AAA sürekli geliştirilmektedir. Ülkede kurulmuş SHS'lerin herbiri kendi uzmanlık alanları ile ilgili olarak elektronik sertifika üretmektedir [84]. Korea Financial Telecommunications & Clearings Institute, Koscom Inc., KTNET, National Computerization Agency, Korea Electronic Certificate Authority ve Korea Information Certificate Authority Inc. SHS olarak ülkede faaliyet göstermektedir [85].

Çizelge 3–3: SHS'ler (G.Kore)

Yetkili SHS'ler	Akreditasyon Tarihi	Faaliyet Alanı
KICA (SignGATE)	10.02.2000	Güvenlik
KOSCOM (SignKOREA)	10.02.2000	Özel sektör
KFTC (yessign)	12.04.2000	Finans
NCA (NIASign)	13.03.2001	Kamu sektörü
CrossCert (CrossCert)	24.11.2001	Web sunucuları
KTNET (TradeSign)	11.03.2002	Elektronik ticaret

SignKOREA, yapılan denetimler doğrultusunda güvenilirliği kanıtlanmış, ülkenin önde gelen SHS'lerinden birisidir. İlk akredite edilmiş SHS konumunda olan SignKOREA, elektronik ticaret, elektronik bankacılık ve sağlık alanlarında 2000 yılından beri hizmet vermektedir. SignKOREA, sertifika hizmeti sağlamak üzere, modern güvenlik teknolojilerinin kullanıldığı güvenli yapılarda faaliyet göstermektedir [86].

İlk akredite SHS'lerden birisi olan SignGATE, kimlik doğrulamasına ve elektronik ortamda güvenli işlem yapılmasına ilişkin hizmetleri sağlamaktadır. SignGATE, elektronik ticaret uygulamalarının güvenliğini teminen elektronik sertifika üretmektedir [82].

Yessign, internet bankacılığı, kredi kartı, sigorta işlemleri gibi alanlarda elektronik sertifika üretmektedir [85]. 24.11.2001 tarihinde akredite edilmiş olan CrossCert, yerel ve uluslararası web sunucuları için elektronik sertifika üretmektedir [87]. 11.03.2002 tarihinde akredite edilmiş olan TradeSign, elektronik ticaret uygulamalarına ilişkin olarak elektronik sertifika üretmektedir [88].

NIASign, kamu sektöründe çalışan kişiler için elektronik sertifika üretmekte, ayrıca elektronik devlet uygulamalarının yaygınlık kazanmasını amaçlamakta ve bu doğrultuda faaliyet göstermektedir. SHS olarak faaliyete başlaması ile birlikte NCA (National Computerization Agency – Milli Bilgisayarlandırma Dairesi), milli ihale sistemini elektronik ortama aktarma çalışmalarını yürütmüştür. Zira NCA, sadece kamu görevlileri için elektronik sertifika üretmek ile kalmamış, aynı zamanda AAA tabanlı uygulamaları da desteklemiştir [84].

3.2.3.4. Sertifika hizmet sağlayıcılarının denetimi

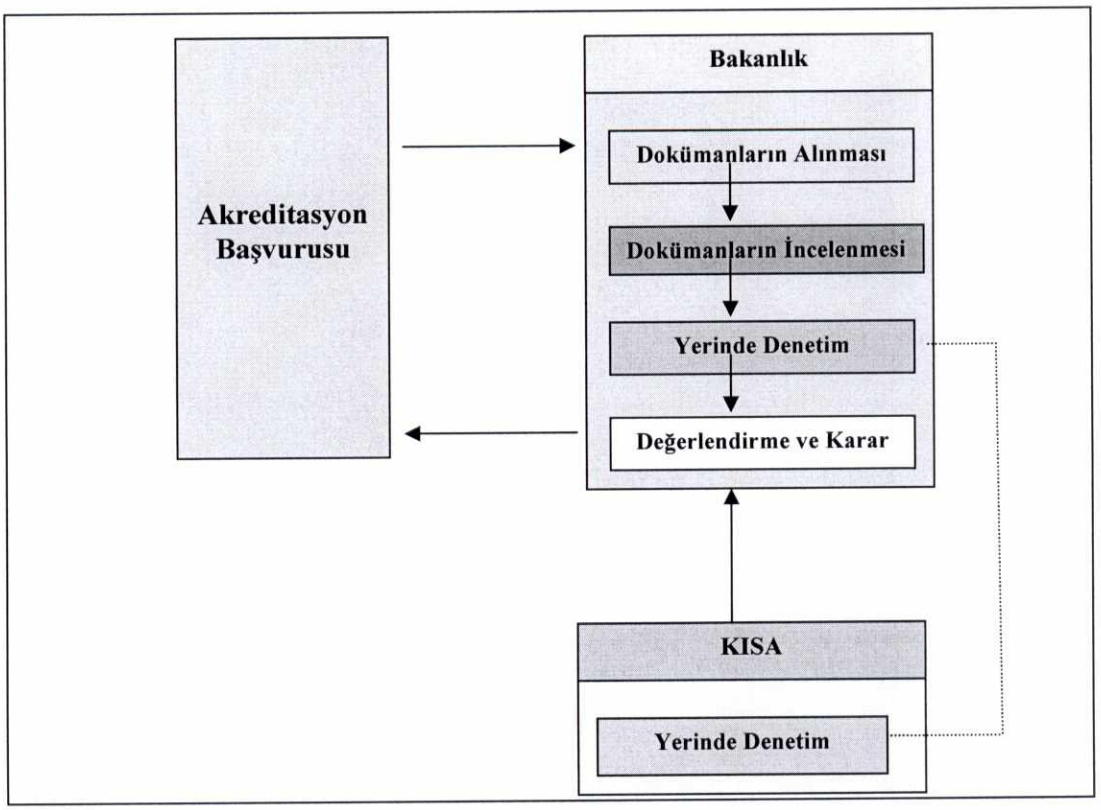
Elektronik İmza Kanununun 4 üncü maddesi uyarınca Bilgi ve İletişim Bakanlığı, sertifikasyon hizmetlerini güvenli ve güvenilir bir şekilde yürütebileceğini ispat eden kurum veya kuruluşları SHS olarak akredite etmektedir. Bilgi ve İletişim Bakanlığının akreditasyon yetkisi zorunlu bir nitelik taşımaktadır. Başka bir deyişle, SHS'ler Bakanlık tarafından akredite edildikten sonra faaliyete geçebilmektedir. SHS olmak için akredite edilmek isteyen kuruluşların elektronik sertifika sağlama faaliyetlerinin sağlıklı bir şekilde yürütülmesi için teknik ve mali yeterliliğe, imkânlara ve donanıma sahip olması gerekmektedir.

SHS'lerin denetimi, SHS olarak faaliyete başlamadan önce ve faaliyete başladıktan sonra olmak üzere iki şekilde gerçekleştirilmektedir. SHS olmak için akreditasyon

başvurusunda bulunan kuruluşlar tarafından, teknik ve mali yeterliliğe, imkân ve donanıma sahip olduklarını belirten ve ayrıntıları yönetmelikte düzenlenmiş dokümanlar Bakanlığa ibraz edilmektedir.

Bakanlık tarafından söz konusu dokümanlar üzerinde yapılan inceleme çalışmalarını müteakip, KISA tarafından yerinde denetim çalışmaları yürütülmektedir. Yapılan denetim çalışmaları sonucunda KISA, bir denetim raporu hazırlamakta ve bu denetim raporunu Bakanlığa sunmaktadır. Bakanlık, KISA'nın denetim raporu çerçevesinde ilgili kuruluşun SHS olarak faaliyete başlayıp başlamayacağına ilişkin kararını vermektedir. SHS olarak akredite edilen kuruluşlara Bakanlık tarafından "akreditasyon belgesi" verilmektedir. Bakanlık tarafından akredite edilen SHS'nin elektronik sertifikası, sertifikasyon uygulamalarına başlamadan önce, KISA tarafından onaylanmaktadır. (Şekil 3–5)

Faaliyete geçen SHS'lerin denetimi KISA'nın münhasır yetkisinde bulunmaktadır. Elektronik İmza Kanununun 25 inci maddesi uyarınca KISA, elektronik imzanın güvenli ve güvenilir bir şekilde kullanılması ve faaliyetlerin güvenli bir şekilde yürütülüp yürütülmediğinin kontrol edilmesi amacıyla akredite edilmiş SHS'leri denetlemektedir. Söz konusu denetimler, KCAC tarafından hazırlanan "Sertifika Hizmet Sağlayıcıları İçin Koruyucu Kurallar" ve denetim sırasında denetim kapsamında yer alan hususları ve bu hususların hukuki dayanağını gösteren "Denetim Rehberi" dokümanları çerçevesinde yürütülmektedir [78].



Şekil 3–5: SHS'lerin denetimi (G.Kore)

4. TÜRKİYE'DE FAALİYET GÖSTEREN ESHS'LERİN DENETİMİNE İLİŞKİN USUL VE ESASLAR

Bağımsız idari otoriteler fonksiyonel olarak, temelde düzenleme yapma yanında, denetleme ve gözetim ve bunun sonucunda yaptırım uygulama konusunda da faaliyet göstermektedir [89]. Bir alan düzenlendiği zaman, o düzenlemelere uygun faaliyette bulunulup bulunulmadığının tespiti için gözetim ve denetim imkânının olması gerekmektedir. Görev alanlarına ilişkin düzenleyici işlem yapma yetkilerinin doğal sonucu olarak, bağımsız idari otoriteler, kanun ve ikincil düzenlemeler ile getirilen kurallara uyulup uyulmadığını izlemek, gözetmek durumundadır. Bu amaçla, bu kuruluşlara, gerekli görülen bilgi ve belgeleri isteme, denetlenen tarafın bilgisine başvurma ve gerektiğinde yerinde inceleme yapma yetkileri verilmiştir [90].

Ticari ve kamusal işlemlerin elektronik ortamda güvenliğini amaçlayan ve elektronik ortamda gerçekleştirilen işlemleri hukuki açıdan geçerli kılması dolayısıyla büyük önem taşıyan 5070 sayılı Elektronik İmza Kanunu 23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiştir. Kanunun ilgili maddeleri doğrultusunda TK tarafından hazırlanan Sertifika Mali Sorumluluk Sigortası Yönetmeliği 26 Ağustos 2004 tarihli ve 25565 sayılı Resmi Gazete'de, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ 6 Ocak 2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

İkincil düzenlemelerin tamamlanmasını müteakip Elektronik Bilgi Güvenliği A.Ş., TÜBİTAK – UEKAE (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), TürkTrust A.Ş. ve e-Tuğra A.Ş. TK'ya bildirimde bulunmuş, ESHS olma vasfını kazanmış, yapılan incelemeler neticesinde mevzuata aykırı bir durum tespit edilmemiş ve bu kurum ve kuruluşlar faaliyete geçmiştir.

Kanunun 15 inci maddesinde, *"Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir. Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur."* hükmü yer almaktadır.

Söz konusu hüküm gereğince TK, ESHS'lerin denetimi konusunda münhasıran yetkili kılınmıştır. TK'nın ESHS'ler üzerindeki denetim yetkisi, söz konusu kuruluşların faaliyete geçmesi ile birlikte başlamaktadır. Ancak Kanunun 21 inci maddesi ile TÜBİTAK-UEAKE denetim dışında bırakılmaktadır.

Kanunun 8 inci maddesi uyarınca ESHS; güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü hukuki ve teknik tedbiri almak ile yükümlü kılınmıştır. Hukuki ve teknik tedbirlerin nasıl alınacağı Kanun, Yönetmelik, Tebliğ ve Tebliğin atıfta bulunduğu standartlardan oluşan elektronik imza mevzuatında belirtilmektedir. Bu düzenlemelerde yer alan hükümler ile Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelikteki düzenlemeler denetim usullerini ve denetim esaslarını teşkil etmektedir.

Tebliğin 5 inci ve 9 uncu maddeleri uyarınca ESHS'nin, işleyişinin bütün aşamalarında ETSI TS 101 456 ve CWA 14167–1 (CEN Workshop Agreement – CEN Çalıştay Kararı) standartlarına uyması gerektiği hüküm altına alınmıştır. Tebliğin 11 inci maddesi uyarınca ESHS'nin TS ISO/IEC 27001 veya ISO/IEC 27001 (International Organisation for Standardisation / International Electrotechnical Commitee – Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi) standardına uygunluğunu yetkili kurum veya kuruluşlardan alınan belgelerle belgelendirmesi gerektiği belirtilmiştir. Her ne kadar ESHS, TS ISO/IEC

27001 veya ISO/IEC 27001 standardına uygunluğunu belgelendirmiş olsa da söz konusu standartta geçen ve ESHS'nin işleyişinde önemli rol oynayan bazı hususların da denetim çalışmaları sırasında dikkate alınmasının gerekli olduğu değerlendirilmektedir.

Bu bölümde, TK'nın kanuni denetim yetkisini kullanma sürecinde ilgili tarafların elektronik imza mevzuatı çerçevesinde dikkate alması gereken denetim usul ve esasları incelenecektir.

4.1. Denetim Usulleri

Yönetmeliğin 4 üncü maddesinde denetim kavramı; ESHS'nin her türlü faaliyet ve işleyişinin ilgili mevzuat hükümlerine uygunluğunun incelenerek; muhtemel hata, noksanlık, usulsüzlük ve/veya suistimallerin tespit edilmesi ve ilgili mevzuatta öngörülen yaptırımların uygulanması amacıyla yapılan çalışmalar bütünü olarak tanımlanmıştır.

Yönetmeliğin 22 nci maddesi ile ESHS'lerin denetiminin TK tarafından gerek görülmesi halinde ve iki yılda en az bir defa re'sen yapılacağı hüküm altına alınmıştır. Yönetmeliğin ilgili maddelerinde, denetim çalışmalarını yürüten ve bu çalışmalar sonucunda denetim raporu hazırlayan TK personeli "denetim görevlisi" olarak tanımlanmış ve denetim usullerine ilişkin düzenlemeler yapılmıştır.

4.1.1. Denetim ilkeleri

Yönetmeliğin 23 üncü maddesinde ESHS'lerin denetiminde uyulması gereken tarafsızlık, özen ve bağımsızlık ilkelerine, 25 inci maddesinde ise gizlilik ilkesine yer verilmiştir. Söz konusu ilkeler, denetim çalışmalarına katılan ilgili taraflar için yol gösterici bir nitelik taşımaktadır. Bu itibarla, aşağıda zikredilen denetim ilkelerinin uygulanması etkin ve verimli bir denetim çalışmasını gerçekleştirmek noktasında büyük önem taşımaktadır.

4.1.1.1. Tarafsızlık ilkesi

Yönetmeliğin 23 üncü maddesinin (a) bendi uyarınca denetim çalışmaları sırasında, sonuçların değerlendirilmesinde ve denetim raporunun hazırlanmasında denetim görevlisinin tarafsız olması gerekmektedir.

Denetim görevlisi, denetim çalışmaları sırasında, tarafsız olmalı, yeterli kanıt toplayıp, ilgili durumları ve mevzuat hükümlerini göz önünde bulundurarak tarafsız bir şekilde karar vermelidir [91]. Denetim görevlisinin, tarafsızlık ilkesi ile bağlantılı olarak, denetim çalışmaları sırasında şeffaf ve adil olmasının yanında ayrımcı olmaması da gerekmektedir.

4.1.1.2. Özen ilkesi

Yönetmeliğin 23 üncü maddesinin (c) bendi uyarınca, denetim faaliyetine ilişkin çalışmaların her aşamasında gerekli özenin gösterilmesi gerekmektedir.

Denetim görevlisinin; çalışmalarını gerekli titizliği göstererek planlamak, programlamak, yeterli miktarda, uygun nitelikte ve güvenilir delil toplamak, delilleri değerlendirmek ve bulguları anlaşılır ve düzenli bir şekilde göstermek, verilerin doğruluğu hakkında dürüst ve doğru bir yargıya ulaşmak ve ulaştığı yargının göstergesi olan görüşünü denetim raporunda açıklamak gibi yükümlülükleri bulunmaktadır [91].

4.1.1.3. Bağımsızlık ilkesi

Bağımsızlık, mesleki faaliyetin dürüst ve tarafsız yürütülmesini sağlayacak bir davranış ve anlayışlar bütünüdür [92]. Yönetmeliğin 23 üncü maddesinin (b) bendi uyarınca dürüstlüğü ve tarafsızlığı etkileyebilecek herhangi bir müdahaleye imkân vermemek ilkesi hüküm altına alınmıştır. Denetim görevlisi, çalışmaları sırasında ortaya çıkabilecek çıkar çatışmalarından uzak kalmak, dürüstlük ve tarafsızlığı etkileyebilecek Kurum içi veya Kurum dışı müdahalelere kapalı olmak, bağımsız

denetim sonucunda ulaştığı görüşlerini, başkalarının doğrudan veya dolaylı çıkarlarını düşünmeksizin raporunda açıklamak zorundadır. Denetim görevlisinin, denetim sürecinde kendi uzmanlığına güven duyarak dış etkenlerin etkisinde kalmadan, yani nesnel düşünerek ve davranarak denetim çalışmalarını yürütmesi gerekmektedir [93].

Bununla bağlantılı olarak, denetim görevlisi ile birinci dereceden akrabalarının; ESHS ile ilgili olanlardan, doğrudan veya dolaylı olarak menfaat temin ettiklerinin ortaya çıkması, ESHS'nin yönetim, denetim veya sermaye bakımından doğrudan veya dolaylı olarak bağlı bulunduğu veya kontrolü altında bulundurduğu gerçek veya tüzel kişilerle ortaklık ilişkisine girmiş olduklarının belirlenmiş olması, ESHS'nin kurucu ortağı olması, yönetim kurulu başkan veya üyesi, genel müdür veya yardımcısı olarak veya karar alma ve uygulama yetki ve sorumluluğu taşıyan başka sıfatlarla görev alması, ESHS ile borçlu-alacaklı ilişkisine girmiş olması, ESHS yetkililerinden önemli sayılabilecek tutarda hediye alması veya özel bir indirimle pay alması durumlarında denetim görevlisinin görevine son verilmesi ve gerekmesi halinde başka bir denetim görevlisinin görevlendirilmesi gerekmektedir [94].

4.1.1.4. Gizlilik ilkesi

Yönetmeliğin 25 inci maddesinin (c) bendi uyarınca denetim görevlisi, denetim çalışmaları süresince edindiği bilgi ve belgelerin gizliliğini sağlamalı ve bunları kanunen yetkili kılınan mercilerden başkasına açıklamamalı ve kişisel yararları için kullanmamalıdır.

4.1.1.5. Etkinlik ilkesi

Denetim çalışmalarının sağlıklı ve verimli bir ortamda yürütülebilmesi bakımından denetim etkinliği hususunun önemli bir yeri bulunmaktadır. Denetim etkinliğini etkileyen birçok faktör bulunmaktadır. Örneğin, denetim görevlisinin, denetim sürecinde sorumluluklarını doğru bir şekilde yerine getirilebilmesi için gerekli teknik bilgiye ve mesleki yeterliliğe sahip olması gerekmektedir [91]. Denetim görevlisi,

denetimin istenen etkinlikte olabilmesini ve denetim sonunda tam ve doğru bir görüş bildirilebilmesini teminen, yapılan işi her seviyede gözden geçirmelidir. Ayrıca, denetim görevlisinin konuyla ilgili tecrübesi ve bilgisi bulunan kişi veya kuruluşlardan görüş alması denetimin etkinliğini etkileyen diğer bir faktördür. Denetimin etkinliğini etkileyen başka bir faktör de, denetim görevlisi tarafından, denetime çıkmadan evvel daha önceki denetim raporlarının dikkate alınması ve daha önceki önerilerin yerine getirilip getirilmediğinin kontrol edilmesidir.

4.1.2. İlgili Daire Başkanlığının denetim işlevleri

TK adına yürütülen denetim çalışmaları sırasında ilgili Daire Başkanlığı, özellikle denetim alanında yıllık hedef ve stratejilerin kesin bir şekilde belirlenmesi, yıllık denetim iş programının hazırlanması ve denetim çalışmalarının planlanması hususlarında önemli bir işlev görmektedir.

Denetimin etkin ve verimli yapılabilmesi açısından, ilgili Daire Başkanlığı tarafından, elektronik imza konusunda yeterli teknik bilgiye ve mesleki yeterliliğe sahip olan kişiler görevlendirilmeli ve denetim görevlisi olarak görevlendirilen kişilere görevlendirmenin amacını ve konusunu gösteren bir yetki belgesi verilmelidir.

Denetim görevlilerinin bilgi, görgü ve yeteneklerinin artırılması ve nitelikli elektronik sertifika pazarındaki yeni denetim yöntemlerinin tanıtılması amacıyla yurt içinde ve yurt dışında denetim görevlilerine eğitim verilmesi, sürekli değişim halinde olan pazarda denetimlerin etkin bir şekilde yapılması noktasında büyük önem taşımaktadır.

Bu itibarla, denetim görevlilerinin eğitimi konusunda ilgili Daire Başkanlığına önemli görevlerin düştüğü değerlendirilmektedir.

4.1.3. Denetim görevlisinin işlevleri

Yönetmeliğin 24 üncü maddesinin (a) bendi uyarınca denetim görevlisi, gerekmesi durumunda, her türlü defteri, belgeyi ve kayıtları istemeye ve incelemeye yetkili olup, Yönetmeliğin 25 inci maddesinin (b) bendi doğrultusunda defter, belge ve kayıtların asıllarını olduğu gibi korumalı ve işin bitiminde ESHS yetkililerine geri vermelidir. Denetim görevlisi; defter, belge ve kayıtlar üzerinde incelemenin gereği olan işaretler dışında şerh, ilave veya düzeltme yapmamalıdır.

Yönetmeliğin 24 üncü maddesi çerçevesinde denetim görevlisi, ESHS'nin yönetim yerlerine, binalarına ve eklentilerine girmeye, bu yerlerde inceleme yapmaya yetkilidir. Bununla bağlantılı olarak denetim görevlisi, denetim ile ilgili olarak yazılı veya sözlü bilgi isteyebilmekte ve gerekli tutanakları düzenleyebilmektedir. Bununla birlikte denetim görevlisinin, denetim çalışmaları sırasında, ESHS'nin yönetim ve yürütme işlerine müdahale anlamına gelebilecek hareket ve davranışlardan kaçınması gerekmektedir.

Denetim çalışmalarının her aşamasında objektif, bağımsız ve tarafsız olması gereken denetim görevlisi, denetim görevini ifa ederken, görevinin ve taşıdığı sorumlulukların gerektirdiği itibarı ve güven duygusunu zedeleyecek türden tutum ve davranışlarda bulunmamalıdır. Diğer bir ifade ile denetim görevlisi, denetim çalışmaları sırasında, doğrudan veya dolaylı olarak ESHS yetkililerinin misafiri konumunda bulunmamalı, ikramlarını kabul etmemeli, ESHS yetkilileri ile borç ilişkisine girmemeli ve hiç bir surette menfaat temin etmemelidir. Bununla bağlantılı olarak, denetim görevlisi, ESHS'nin yönetici ve çalışanlarına karşı ciddi, vakarlı ve soğukkanlı bir tutum içerisinde bulunmalı ve söz konusu kişilerle gereksiz tartışmalardan kaçınmalıdır.

Ayrıca, denetim sırasında edinilen ve ticari sır niteliğini taşıyan bilgileri kanunen yetkili kılınan kişilerden başkasına açıklamamalı ve doğrudan veya dolaylı şekilde kendisi ya da üçüncü kişilerin yararına kullanmamalıdır.

Denetim görevlisi, yapılan denetim çalışmaları neticesinde, elektronik imza mevzuatına aykırılık teşkil eden uygulamaların ve eksikliklerin giderilmesi ve düzeltilmesi yollarını araştırmalıdır.

4.1.4. ESHS'nin denetim işlevleri

Denetim sürecinde denetim görevlisinin olduğu kadar ESHS'nin de denetim işlevleri bulunmaktadır. Yönetmeliğin 26 ncı maddesi ile ESHS, denetim görevlilerinin yetkileri çerçevesindeki taleplerini en kısa sürede karşılamakla ve denetim görevlilerine elverişli bir çalışma ortamı sağlamakla yükümlü kılınmıştır. Söz konusu maddenin devamında ESHS'nin, gizlilik ve sır saklama gibi gerekçeler ileri sürerek denetim yükümlülüklerinden imtina edemeyeceği hüküm altına alınmıştır.

ESHS'nin gerçekleştirdiği faaliyetlerin mevzuata uygun olup olmadığının tespit edilebilmesi için ESHS'ye ait yönetim yerlerinin, binaların ve eklentilerinin, sistem, cihaz, yazılım ve donanımların denetim görevlisinin erişimine açık tutulması gerekmektedir. Bu durumla bağlantılı olarak ESHS, denetimi sağlayıcı gerekli altyapıyı temin etmeli ve çalışır vaziyette bulundurmalıdır.

Denetim görevlisi tarafından yürütülen çalışmaların sonucunda tespit edilen mevzuata aykırılık hallerinin ESHS tarafından en kısa süre içinde giderilmesi gerekmektedir.

4.1.5. Denetim süreci

Denetim görevlisi, denetimin etkin ve sağlıklı bir şekilde yapılabilmesi için, denetim çalışmalarına başlamadan önce görevlendirme konusu ile ilgili olarak hazırlık çalışmaları yapmalıdır. Bu çerçevede, öncelikle elektronik imza mevzuatı taraması yapılmalı, geçmişte hazırlanmış denetim raporları incelenmeli, bu raporlarda belirtilen hususların yerine getirilip getirilmediği kontrol edilmeli ve ESHS'nin kurumsal yapısı ve iş ilişkisi içinde olduğu üçüncü kişiler hakkında bilgi toplanmalıdır.

Çalışmaların ekip halinde yapılması durumunda, ekibe dahil olan denetim görevlilerinden ilgili Daire Başkanlığının personeli arasında unvan olarak en yüksek olan kişinin, aynı unvanda birden fazla kişi olması halinde ise bu unvanda hizmet yılı en fazla olan denetim görevlisinin ekip başkanı olarak belirlenmesi gerekmektedir. Ekip başkanı, denetim sürecinin yönünün belirlenmesine, işlerin seyrinin takip edilmesine ve sonuç alınmasına ilişkin fikir ve tedbirlerin uygulanmasını temin etmek üzere denetim çalışmalarını koordine etmelidir.

TK, ESHS'lerin denetimini re'sen veya kendisine intikal eden ihbar veya şikâyet üzerine yapmaktadır. Denetim çalışmaları, ilgili Daire Başkanlığı tarafından görevlendirilen personel vasıtasıyla yürütülmekte, ilgili Daire Başkanlığı tarafından yapılan görevlendirme neticesinde görevlendirilen personel *denetim görevlisi* vasfını kazanmaktadır.

Yönetmeliğin 25 inci maddesinin (a) bendi uyarınca denetim görevlisi denetime başlamadan önce denetim görevlisi olduğuna dair belge ile kendisini tanıtmakla yükümlü kılınmıştır. Bu çerçevede denetim görevlisi, göreve başlamadan önce Kurum adına denetim yetkisini haiz olduğuna dair görevlendirme yazısı veya kimlik belgesi ile kendisini ESHS'ye tanıtmalıdır.

Sistematik bir süreç olan denetim süreci, denetim görevlisinin görevlendirilmesiyle başlayan ve yapılacak planlama doğrultusunda uygulanacak olan denetim yöntemleri ile faaliyetlerin test edilmesi sonucu toplanan deliller çerçevesinde değerlendirme ve raporlama aşamalarını kapsayan bir süreçtir [91]. Bu sürecin etkin ve verimli bir şekilde yürütülmesi için denetim çalışmalarının planlanması, yürütülmesi ve yapılan çalışmaların titiz bir şekilde raporlanarak ilgili birimlere sunulması gerekmektedir.

Denetim sürecini teşkil eden planlama, inceleme, ön araştırma ve soruşturma aşamaları elektronik imza mevzuatında düzenlenmemiştir. Ön araştırma ve soruşturma aşamaları için, gerek görülmesi halinde, Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelikte yer alan hükümler uygulanabilmektedir. Aşağıda ESHS'lerin denetiminde uygulanması

gerektiği değerlendirilen söz konusu aşamalarla ilgili hususlar incelenmiş, bu hususlarla ilgili önerilere beşinci bölümde yer verilmiştir.

Denetim süreci, üç temel aşamayı içermektedir [31]:

- Planlama
- Denetim çalışmalarının yürütülmesi
- Raporlama

4.1.5.1. Planlama

Planlama, herhangi bir sonuca varılmasını teminen yeterli ve uygun delillerin toplanması noktasında işlev gördüğü için önemli bir aşamadır [95]. Denetim çalışmalarına başlamadan önce düzgün bir planlamanın yapılması, denetim çalışmalarının sağlıklı bir şekilde yürütülmesini önemli ölçüde etkileyecektir. Zira planlama aşaması ile ESHS'nin denetimi sonucunda oluşturulacak denetim görüşüne ulaşmak için izlenecek yol ve yöntem belirlenmektedir [31].

Denetim çalışmalarının düzenli ve verimli bir şekilde yürütülebilmesi için denetim planının hazırlanması büyük önem taşımaktadır. Denetim planı, denetim süreci için yol haritası niteliğindedir [96]. Denetim planı; denetim görevlisinin denetim çalışmalarını yönlendirmesinde ve yönetmesinde izleyeceği stratejiyi içermekte ayrıca denetim görevlisinin, ESHS'yi tanımasını ve muhtemel riskleri tanımlayabilmesini sağlamaktadır. Buna göre, gerçekleştirilecek denetimin ne nitelikte ve kaç kişilik bir ekiple, ne kadar zamanda ve hangi noktalara yoğunlaşılarak yapılacağı ortaya konmuş olmaktadır.

Bu itibarla, bir denetim görevlisi için denetimin etkin ve verimli olabilmesinin öncelikli koşulu, denetimin iyi planlanmış olmasıdır. Karşıt olarak iyi planlanmamış bir denetim, belirli noktaların gözden kaçmasına, özensizliğe, sonuçta denetim etkinliğinin zayıflamasına yol açacaktır. Bu durum, denetim görevlisinin ESHS'nin

denetimine ilişkin yargısının ve görüşünün denetim raporuna eksik yansıması anlamına gelmektedir [93].

Denetim rehberi, ESHS'nin denetime konu olan faaliyetlerinin tespit edilmesi noktasında oldukça önemli bir yer tutmaktadır. Denetim planının, denetim rehberi çerçevesinde tespit edilen konular dikkate alınarak oluşturulmasının, denetim çalışmalarının sağlıklı, etkin ve verimli sonuçlar doğurması bakımından oldukça önemli olduğu değerlendirilmektedir. Zira denetim rehberinden elde edilecek bilgiler dikkate alınarak, denetim işinin ne kadar sürede tamamlanabileceğine yönelik bir zaman planlamasının ve aynı zamanda ne kadar insan kaynağına ihtiyaç duyulacağı ile ilgili bir işgücü planlamasının yapılması mümkün olmaktadır.

Denetim rehberi; denetim ile amaçlanan hususları belirgin hale getirmekte, denetim düzenini ve sürekliliğini temin etmekte, denetim görevlisinin denetim kapsamından çıkmasını önlemekte ve denetim çalışmaları sırasında denetim görevlisinin iş yükünü hafifletmektedir [97]. Denetim rehberinin, elektronik imza mevzuatında yer alan ve ESHS'lerin yerine getirmekle yükümlü olduğu bütün hususları kapsaması gerekmektedir.

4.1.5.2. Denetim çalışmalarının yürütülmesi

Denetim çalışmaları; inceleme, ön araştırma ve/veya soruşturma aşamalarından oluşmaktadır. İnceleme aşaması, denetim çalışmalarının temelini oluşturmaktadır. Çünkü bu aşama, denetim sonucunu etkileyen ve gerekli ve yeterli delillerin toplandığı aşamadır. Ön araştırma ve soruşturma aşamaları ise yapılan incelemeler neticesinde gerekmesi durumunda yürütülen ve denetim sürecinin diğer önemli unsurlarını teşkil eden aşamalardır.

4.1.5.2.1. İnceleme

Denetim genel anlamda, bir delil toplama ve bu delilleri değerlendirme faaliyetidir [36]. İnceleme aşaması, ESHS'nin denetime tabi faaliyetlerinin ilgili mevzuata

uygun olup olmadığını tespit etmek üzere dosya üzerinde ve/veya yerinde yapılan incelemeleri kapsamaktadır. Bu kapsamda, denetim planı çerçevesinde inceleme çalışmaları yapılmakta ve gerekli deliller elde edilmektedir.

Denetim görüşünün oluşturulmasına esas teşkil edecek deliller belirli yöntemlere başvurularak elde edilmektedir. Denetim görevlisinin, ESHS'nin aleyhine olan delillerin yanında lehine olan delilleri de dikkate alması hakkaniyetin bir gereğidir. Denetim görevlisinin, topladığı delilleri tutanak ile ESHS'nin imzaya yetkili yöneticisine imzalatması, imzadan kaçınılması halinde denetim görevlisi tarafından buna ilişkin tutanak hazırlanması gerekmektedir.

Denetim delilleri, denetim yöntemlerinin uygulanması sonucu ortaya çıkarılan denetime yönelik ürünlerdir. Denetim görevlisinin, incelemelerini yürütürken aşağıda belirtilen yöntemlerden bir veya birkaçını uygulayarak, güvenilir sonuçlar çıkarmaya elverişli, uygun ve yeterli miktarda olan denetim delillerini toplaması gerekmektedir.

- Fiziki İnceleme Yöntemi: Fiziki inceleme, belgelerde ve kayıtlarda gösterilen fiziki kıymetlerin gerçekten var olduklarının görülmesi ve varlığı saptanan kıymetlerin ESHS'ye ait olduğunun resmi belge ve kayıtlarla doğrulanması işlemidir [98]. Bu yöntem, ESHS envanterinde kayıtlı olan varlıkların gerçekte var olup olmadıklarının anlaşılabilmesi için kullanılan bir yöntemdir. Söz konusu yöntem uygulanırken, resmi belgeler ve maddi varlıklar kullanılarak, bunların uygunluğu kontrol edilmektedir. ESHS'ye ait belgelerin doğruluğunun tespit edilmesi açısından fiziki inceleme önemli bir araçtır. Bu yöntem sayesinde maddi kıymetlerin varlığı ve durumu hakkında doğrudan bilgi edinilmektedir [31].

- Gözlem Yöntemi: Gözlem; işlemlerin nasıl ve ne şekilde yapıldığının araştırılmasını ifade eder [91]. Diğer bir ifade ile gözlem, denetim süresince ESHS faaliyetlerinin ve bu faaliyetlere ilişkin iş akışlarının gözlenip izlenmesi olarak adlandırılır [31]. Gözlemin konusu, kişiler, işlemler ve süreçlerdir. Özellikleri itibariyle uygulama aşamasında belirli tespitlerin

yapılmasını gerekli kılan işlemlerde gözlem yoluyla güvenilir deliller elde edilmektedir. Doğrudan denetim görevlisi tarafından toplanan bilgilerin güvenilirlik derecesi yüksektir. Bu yöntem sayesinde; ESHS için öngörülen kurallara uyulup uyulmadığına, iç kontrol süreçlerinin etkinliğine, toplanan verilerin gerçek duruma uygunluğuna ve dolayısıyla toplanan bilgi ve belgelerin doğruluğuna ilişkin hususları kontrol etme imkanı elde edilmektedir.

- Doğrulama Yöntemi: Doğrulama; denetim görevlisinin belirlediği çerçevede, ESHS dışındaki bir kaynaktan ESHS'nin yazılı talebiyle bilgi istenmesi ve bu bilginin doğrudan denetim görevlisine iletilmesi işlemidir [91].

- Göz Atma Yöntemi: Göz atma, denetim görevlisine doğrudan delil toplama imkanı vermeyen, hangi işlem ve kayıtların daha dikkatlice inceleneceği hususunda bilgi veren bir yöntemdir [38]. Denetim görevlisine, soruşturma kapsamında özel nitelikteki bazı hususların incelenmesi görevi verildiğinde ilgili hususların derinlemesine incelenmesi gerekir. Ancak, ESHS'nin genel denetimi yapılırken, derinlemesine incelemeyi gerektirecek önemli sapmalar gösteren kalemlerin tespit edilmesi amacıyla, ilgili mali tablolara, muhasebe kayıtlarına ve diğer belgelere göz atılabilir [31]. Böylece denetim görevlisi tarafından öncelikle incelenmesinde fayda görülen hususlar tespit edilmektedir.

- Soru Sorma Yöntemi: Soru sorma, ESHS'nin faaliyetlerine ilişkin olarak ESHS personelinden veya ESHS dışındaki bağımsız kişi ve kuruluşlardan sözlü ve yazılı bilgi alınmasıdır [31]. İlgililere yöneltilecek sorular, ESHS'nin faaliyetleri ile ilgili olarak denetim görevlisi tarafından bilinmesine ihtiyaç duyulan hususlara yöneliktir. Soruların amaca yönelik olması ve uygun kişi veya makama yöneltilmesi, soruların ilgilileri rencide edici veya aşağılayıcı ifadeler içermemesi önem taşımaktadır. Elde edilen cevapların raporlama aşamasında delil oluşturması bakımından sorulan sorularla, sorulara karşılık

alınan cevapların ilgililerin imzasını taşıyan tutanağa bağlanması gerekmektedir [93].

- Belge İnceleme Yöntemi: Belge incelemesi; ESHS'nin yürütmüş olduğu faaliyetlere ilişkin her türlü belgenin içeriğinin ve kayıtlara uygunluğunun ayrıntılı şekilde incelenmesi işlemidir [98]. Belgelerin incelenmesi sırasında, bu belgelerin mali, ticari ve hukuki açılardan değerlendirilmesi gerekmektedir [91]. İncelenecek belgeler; uygulama dokümanları, fatura, sigorta poliçeleri, teslim ve tesellüm makbuzları, ücret bordroları, sözleşme, taahhütname, kefaletname, mahkeme ilamı gibi varlık, hak, alacak ve yükümlülükleri tevsik eden türden belgeler olabilmektedir. Belgelerin maddi ve şekli yönden incelenmesinde doğrudan belgelerin kendisi hedef alınmalıdır.

Yukarıda belirtilen yöntemlerin bir veya birkaçı kullanılarak yapılan incelemeler sonucunda, ESHS'nin faaliyetlerinin soruşturma aşamasını gerektirmeyecek şekilde ilgili mevzuat hükümlerine açıkça aykırılığının tespit edilmesi ile elde edilen deliller doğrultusunda inceleme raporunun hazırlanması, Kurula sunulması ve Kurulun ilgili mevzuat hükümleri çerçevesinde ESHS ile ilgili kararını vermesi gerekmektedir.

4.1.5.2.2. Ön araştırma

Ön araştırma, denetlenen taraf hakkında soruşturma açılmasına gerek olup olmadığının tespiti için öngörülen bir ara süreçtir.

Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmeliğin 40 ıncı maddesinde *"Kurul, ilgili kanunlarla ve işbu Yönetmelikle belirlenen görevleri ile ilgili olarak re'sen veya kendisine intikal eden ve işletmeciler, aboneler, kullanıcılar ve Türk telekomünikasyon sektöründe yer alan tüm gerçek ve tüzel kişilerin ilgili mevzuata ve lisanslara aykırı faaliyetleri ile ilgili başvurular ve şikayetler üzerine doğrudan soruşturma açılmasına ya da soruşturma açılmasına gerek olup olmadığının tespiti için ön araştırma yapılmasına karar verir.*

Ön araştırma yapılmasına karar verildiği takdirde Kurul, Kurum çalışanlarından bir ya da birkaçını görevlendirir. Ön araştırma yapmakla görevlendirilen Kurum çalışanları 30 gün içinde elde ettiği bilgileri, her türlü delilleri ve konu hakkındaki görüşlerini Kurula yazılı olarak bildirir." hükmü,

41 inci maddesinde ise *"Ön araştırma raporunun Kurula teslimini takip eden 10 gün içinde, Kurul elde edilmiş olan bilgileri değerlendirerek karar vermek üzere toplanır ve soruşturma açılmasına veya açılmamasına karar verir."* hükmü yer almaktadır.

Söz konusu madde hükümlerinden; ön araştırma yapılmasına Kurulun karar verebileceği ve ön araştırma yapılmasına karar verildiği takdirde Kurulun, Kurum çalışanlarından bir ya da birkaçını görevlendireceği sonucu çıkmaktadır.

Ancak, denetim çalışmalarının etkinliği açısından, Kurul tarafından ön araştırma için ilgili Daire Başkanlığının görevlendirilmesi ve ilgili Daire Başkanlığı tarafından yapılacak görevlendirme ile "denetim görevlisi" vasfını kazanan personel tarafından hazırlanacak denetim raporunun Kurula sunulması suretiyle ön araştırma aşamasının düzenlenmesi gerekmektedir.

4.1.5.2.3. Soruşturma

Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmeliğin 42 nci maddesinde *"Kurul tarafından soruşturma yapılmasına karar verildiği takdirde; Kurul tarafından, soruşturma yapmak üzere Kurum Başkan Yardımcısı veya Daire Başkanlarından birinin başkanlığında Kurum personelinden oluşan bir heyet görevlendirilir. Soruşturma en geç 3 ay içinde tamamlanır. Gerekli görüldüğü hallerde bir defaya mahsus olmak üzere Kurul tarafından 3 aya kadar ek süre verilebilir."* hükmü yer almaktadır.

Kurul tarafından, ön araştırma raporu neticesinde veya doğrudan soruşturma açılmasına karar verildiği takdirde, soruşturma aşamasına geçilmektedir. Söz konusu Yönetmeliğin 42 nci maddesi kapsamında, Kurulun, soruşturma yapmak üzere

Kurum Başkan Yardımcısı veya Daire Başkanlarından birinin başkanlığında Kurum personelinden oluşan bir heyeti görevlendireceği hüküm altına alınmıştır. Ancak, inceleme ve ön araştırma aşamalarında olduğu gibi soruşturma aşamasında da denetim görevlisinin etkin olması gerektiği değerlendirilmektedir. Diğer bir deyişle, Kurulun, soruşturmayı yürütmek üzere ilgili Daire Başkanlığını, ilgili Daire Başkanlığının, denetim görevlisi vasfını kazanan personeli görevlendirmesi ve denetim görevlisinin denetim raporunu hazırlaması gerekmektedir.

Soruşturma raporu ve ESHS'nin yazılı savunmasından oluşan soruşturma dosyasının denetim görevlisi tarafından ivedilikle değerlendirilmesi, söz konusu değerlendirme sonucunda denetim görevlisinin, gerekmesi durumunda, ESHS hakkında idari yaptırım ve tedbirlerin uygulanmasına ilişkin kanaatini soruşturma raporuna derc etmesi, ilgili Daire Başkanlığı amirinin soruşturma raporunu Kurula sunması ve Kurulun idari yaptırım ve tedbirlerin uygulanmasına veya uygulanmamasına karar vermesi gerekmektedir.

4.1.5.3. Raporlama

Yönetmeliğin 27 nci maddesinde *"Denetim görevlileri tarafından hazırlanan denetim raporu, denetim faaliyetinin sona ermesinden itibaren otuz (30) gün içinde Kurula sunulur."* hükmü yer almaktadır. Yukarıda çerçevesi çizilen denetim sürecinin sonucunda denetim görevlisi, denetime tabi faaliyetlerin ilgili mevzuata uygun olup olmadığını tespit etmek üzere topladığı delilleri değerlendirmesi ve gerekmesi halinde denetim raporunu hazırlaması gerekmektedir.

Denetim görevlisinin hazırladığı denetim raporu eksiksiz olmalı, diğer bir deyişle, görevin gerektirdiği inceleme ve tespitler tam olarak yapılmış ve elde edilen bilgiler, görüş ve sonuçlar ilgili rapora eksiksiz olarak yansıtılmış olmalıdır. Bununla bağlantılı olarak, rapor doğru olmalı [95], sağlam delillere dayanmalıdır. Zira raporun kısmen hatalı olması, raporun tamamı hakkında şüphe oluşturmakla beraber denetim görevlisinin ayrıca saygınlığını da zedelemektedir.

Denetim raporunun amacı, ESHS'yi suçlu bulmak veya cezalandırmak değil, incelenmesi istenilen konuyla ilgili gerçek durumu ortaya çıkarmaktır. Bu nedenle, denetim raporu yapıcı olmalı, ESHS'ye faaliyetlerinde yol gösterecek düzeltici, bilgilendirici ve geliştirici nitelikleri de haiz olmalıdır. Bu itibarla, denetimde saptanan hususlarla ilgili olarak ilgililerle görüşülüp, mevzuat hükümlerinin uygulanmasında uyarıcı, yol gösterici ve öğretici olunması sağlanmalıdır.

Denetim çalışmaları sonucunda denetim raporuna alınması uygun görülen hususlar açık ve ayrıntılı bir şekilde yazılmalıdır. Denetim raporunda yer alan değerlendirmeler olay ve gözlemlere dayandırılmalı, denetim konusu ile ilgisi olmayan hususlara denetim raporunda yer verilmemelidir. Denetim raporunda gereksiz tekrarlardan kaçınılmalı ve rapor içinde yapılan değerlendirmeler arasında uyum gözetilmelidir [95].

Kolayca okunup anlaşılması için denetim raporunun açık ve akıcı bir dille yazılması gerekmektedir [97]. Açıklık kavramı, gereksiz teknik dilden kaçınılarak ve gerekli yerlerde destekleyici bilgiler sağlanarak geliştirilebilir. Ayrıca, hazırlanan raporun; adları raporda geçen kişi veya kuruluşları rencide edebilecek sıfat ve sözler kullanılmaksızın oluşturulması ve konuyla ilgili olmayan ayrıntılardan kaçınılarak düzenlenmesi esastır [99].

4.1.6. İdari yaptırım ve tedbirlerin uygulanması

Kanunun 18 inci maddesinde çeşitli hususlara ilişkin yükümlülüklerini yerine getirmemesi durumunda ESHS'lere verilecek idari para cezaları düzenlenmiştir. 19 uncu maddede ise 18 inci maddedeki suçları işleyen ESHS'lerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri hâlinde para cezalarının iki kat olarak uygulanacağı, üçüncü kez işlemeleri hâlinde ise TK tarafından ESHS'ler hakkında kapatma cezası verileceği hüküm altına alınmıştır.

Ayrıca Kanunun 8 inci maddesi uyarınca, ESHS'nin faaliyetinin devamı sırasında güvenli ürün ve sistemlerin kullanılmasına, hizmetin güvenilir bir biçimde

yürütülmesine ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbirin alınmasına ilişkin şartları kaybetmesi hâlinde TK'nın, bu eksikliklerin giderilmesi için, ESHS'ye bir ayı geçmemek üzere bir süre vereceği, bu süre içinde ESHS'nin faaliyetlerini durduracağı ve sürenin sonunda eksikliklerin giderilmemesi halinde ESHS'nin faaliyetine son vereceği düzenlenmiştir.

Yönetmeliğin 28 inci maddesi uyarınca, denetim raporunda, ilgili mevzuat hükümlerine aykırılık tespit edilmiş olması ve bu tespitin Kurul tarafından da sabit görülmesi halinde, ilgili mevzuatta öngörülen yaptırım ve cezaların uygulanmasına karar verileceği hüküm altına alınmıştır. Kurul, yapacağı incelemeler neticesinde elektronik imza mevzuatı hükümlerinin ihlal edildiğini tespit etmesi halinde mevzuatta belirtilen idari yaptırım ve tedbirlerin uygulanmasına karar vermesi gerekmektedir.

İdari yaptırım ve tedbirlerin uygulanmasına karar verilirken bazı hususların dikkate alınması gerektiği değerlendirilmektedir. Örneğin, benzeri durumlarda benzer suçları işleyen ESHS'lere getirilecek müeyyidelerin uygulanmasında ayrımcılık yapılmaması ve şeffaf olunması gerekmektedir. Yaptırım uygulanmasında ihlalin koşulları ve söz konusu ihlalin kasten veya dikkatsizlik veya ihmal sonucu yapılıp yapılmadığı da göz önünde bulundurulmalıdır. İhlalde bulunan ESHS'nin önceki ihlalleri, ihlalden önce ve ihlalden sonra sergilediği tutum ve davranışlar, idari yaptırımların tespitinde belirleyici olmalıdır [100].

4.2. Denetim Esasları

Kanunun 15 inci maddesinin birinci fıkrasında *"Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir."* hükmü yer almaktadır. ESHS'lerin Kurum tarafından denetlenmesine esas teşkil edecek hususların belirlenmesi adına öncelikle söz konusu kuruluşların *"Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin"* neler olduğunun tespit edilmesi gerekmektedir.

Bu bölümde ESHS'lerin mevcut işleyiş süreçleri incelenecek ve denetime esas teşkil eden hususlar açıklanacaktır. Bu hususlar, ESHS'lerin denetiminde incelenmesi gereken noktaları ve dolayısıyla Denetim Rehberinin kapsamını belirleyecektir.

4.2.1. ESHS uygulama dokümanları

Sİ (Sertifika İlkeleri), SUE (Sertifika Uygulama Esasları) ve BGİ (Bilgi Güvenliği İlkeleri) dokümanları ESHS'nin faaliyetlerinde yol gösterici bir nitelik taşımaktadır. Bu nedenle ESHS'nin, öncelikle söz konusu dokümanları mevzuata uygun bir şekilde hazırlaması ve ilgili tarafların bilgisine sunması gerekmektedir.

4.2.1.1. Sertifika ilkeleri ve sertifika uygulama esasları

Yönetmeliğin 4 üncü maddesinde Sİ, ESHS'nin işleyişi ile ilgili genel kuralları içeren belgeyi ifade etmektedir. Bir başka tanımlamaya göre Sİ, elektronik sertifikaların herhangi bir gruba uygulanabilirliğini nitelemektedir [101].

Sİ; elektronik sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve iptal işlemleriyle ilgili tüm idari, teknik ve yasal gereklilikleri ortaya koymakta ve ilgili tarafların uygulamalara ilişkin sorumluluklarını belirlemektedir.

Yönetmeliğin 4 üncü maddesinde SUE, Sİ'de yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belge olarak tanımlanmaktadır. Bir başka deyişle, SUE, ESHS'nin elektronik sertifika üretme, yönetme ve iptal etme uygulamalarını içeren kurallar bütünü olarak tanımlanmaktadır [101]. SUE, Sİ'de belirlenen kurallara ilgili tarafların nasıl uyduğu, bu gerekliliklerin nasıl hayata geçirildiğini açıklamaktadır. ESHS, Sİ uyarınca uymakla yükümlü olduğu koşulları, SUE'de belirtilen faaliyetler ile yerine getirmektedir [102].

Tebliğin 7 nci maddesi uyarınca ESHS'nin; Sİ'yi ve SUE'yi IETF RFC 3647 (Internet Engineering Task Force Request for Comments – İnternet Mühendisliği

Görev Grubu Yorum Talebi)'ye uygun olarak hazırlaması gerekmektedir. Sİ'de ve SUE'de, elektronik sertifika hizmetlerinin sağlanmasında önemli bir yere sahip olan "güvenilirlik" kavramına ilişkin koşulların nasıl yerine getirildiğinin belirtilmesi, sertifika hizmetlerinde kullanılacak uygulama süreçlerinin açıklanması ve ESHS'nin bazı hizmetlerini dışarıdan sağlayan kurum veya kuruluşların yükümlülüklerinin düzenlenmesi gerekmektedir.

ESHS'nin, Yönetmeliğin 14 üncü maddesi doğrultusunda Sİ ve SUE dokümanlarını en az yirmi yıl süreyle saklaması gerekmektedir. Ayrıca, ESHS, SUE'nin sertifika sahibini veya üçüncü kişileri ilgilendiren bölümlerini ve Sİ'yi internet sayfasında yayımlamakla yükümlü kılınmıştır. ESHS, SUE'yi ve Sİ'yi sertifika sahiplerinin ve üçüncü kişilerin erişimine açık tutabilmekle birlikte, SUE'nin tüm ayrıntılarını herkesin erişimine açmasına yönelik bir yükümlülüğü bulunmamaktadır.

SUE'de yapılması planlanan değişikliklerin önceden açıklanması, söz konusu değişikliklerin ESHS'nin onay biriminden geçirilmesi ve yenilenmiş SUE'nin sertifika sahiplerinin ve üçüncü kişilerin bilgisine sunulması gerekmektedir [103].

4.2.1.2. Bilgi güvenliği ilkeleri

BGİ dokümanı ile, ilgili mevzuat hükümleri ve iş gerekleri uyarınca ESHS yönetiminin bilgi güvenliği hususundaki desteğinin ve yönlendirmesinin sağlanması amaçlanmaktadır. BGİ dokümanı, güvenlik ilkelerinin ve prensiplerinin açıklandığı, bilgi güvenliğinin sağlanmasına ve desteklenmesine ilişkin faaliyetlerin yürütülmesinde büyük önem taşıyan bir uygulama dokümanıdır.

ESHS yönetimi, BGİ'yi ESHS'nin bütün çalışanlarının bilgisine sunmalı ve söz konusu ilkelerin gelişimine ilişkin çalışmaları koordine etmelidir. Söz konusu doküman çerçevesinde belirtilen ilkelerde önemli değişikliklerin meydana gelmesi halinde, dokümanın gözden geçirilmesi gerekmektedir [103].

4.2.2. Anahtar yönetimi yaşam çevrimi

AAA, asimetrik anahtarlama yöntemine dayanan elektronik sertifikaların oluşturulması, değiştirilmesi ve kullanılması noktalarında işlev gören hiyerarşik bir sistemdir. AAA kapsamında gizli anahtar, imzalama ve doğrulama aşamalarında, elektronik sertifika ise elektronik imzanın doğrulanması ve açık anahtarın dağıtılmasında kullanılmaktadır [104].

Anahtar yönetimi; açık anahtarlı şifrelemede ilgili taraflara farklı anahtar çiftinin verilmesi, açık anahtarların herkesin erişimine açık olarak saklanması ve gizli anahtarların mutlak gizliliğinin sağlanmasından sorumlu düzen olarak tanımlanmaktadır [3].

Bu bölümde kullanıcının ve ESHS'nin anahtar yönetimi yaşam çevrimine ilişkin hususlar ele alınacaktır.

4.2.2.1. Kullanıcı anahtar yönetimi yaşam çevrimi

Kanunun 10 uncu maddesinin (d) bendinde ESHS, imza oluşturma verisinin ESHS tarafından veya ESHS'ye ait yerlerde sertifika talep eden kişi tarafından üretilmesi durumunda bu işlemin gizliliğini sağlamakla veya ESHS'nin sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini temin etmekle yükümlü kılınmıştır.

Söz konusu madde hükmü çerçevesinde, kullanıcıya ait gizli anahtarın üretilmesinde iki farklı durum öngörülmüştür. Birinci durum, gizli anahtarın ESHS'ye ait yerlerde üretilmesi durumudur. Bu kapsamda, gizli anahtarın ESHS veya kullanıcı tarafından ESHS'ye ait yerlerde üretilmesi halinde bu işlemin gizliliğini sağlamak ESHS'nin yükümlülüğü altındadır. İkinci durum ise gizli anahtarın ESHS'nin sağladığı araçlarla üretilmesi durumudur. Bu çerçevede, gizli anahtarın ESHS'nin sağladığı araçlarla üretilmesi halinde gizli anahtarın başkaları tarafından kopyalanması ihtimaline karşın ESHS, işleyişin güvenliğini sağlamak ile yükümlü kılınmıştır [105].

Ayrıca, Yönetmeliğin 15 inci maddesi uyarınca kullanıcı; anahtar çiftini ESHS'ye ait olmayan yerlerde ve araçlarla üretebilmektedir. Bu durumda kullanıcı, Tebliğde belirlenen algoritmaları ve parametreleri kullanmakla yükümlü kılınmıştır.

Tebliğin 6 ncı maddesi uyarınca, imza sahibine ait gizli ve açık anahtarların;

- RSA (Rivest-Shamir-Adleman) için en az 1024 bit veya
- DSA (Digital Signature Algorithm – Sayısal İmza Algoritması) için en az 1024 bit veya
- DSA Eliptik Eğrisi için en az 163 bit olması

gerekmektedir.

ESHS'nin, kullanıcılara ait gerek gizli gerekse de açık anahtarın güvenli bir şekilde üretilmesine ve gizli anahtarın gizliliğinin sağlanmasına ilişkin Direktif Ek II (f) maddesinde de bu yönde bir düzenleme yapılmıştır. Bu hüküm doğrultusunda ESHS, kullanıcı anahtarları için güvenli elektronik imzanın kullanım amaçlarına uygun olan ve elektronik imza mevzuatı hükümleri çerçevesinde bir açık anahtar algoritmasını kullanmalıdır.

ESHS tarafından üretilen kullanıcı anahtarları güvenli bir şekilde üretilmeli ve depolanmalıdır. Gizliliği, bütünlüğü ve sadece kullanıcının zilyetliğinde olması sağlanan gizli anahtarın kullanıcıya teslim edilmesi gerekmektedir [26].

Direktif Ek II (j) bendi ESHS'yi, kullanıcıya ait gizli anahtarın kopyalarının bulunması halinde bunları imha etmekle yükümlü kılmış ve bu çerçevede, Kanunun 10 uncu maddesinde ESHS tarafından üretilen gizli anahtarın bir kopyasının alınmaması veya bu verinin saklanmaması yönünde düzenleme yapılmıştır.

4.2.2.2. ESHS anahtar yönetimi yaşam çevrimi

ESHS anahtar yönetimi yaşam çevrimi; gizli anahtarın oluşturulması, kullanılması, saklanması ve yedeklenmesi, açık anahtarın dağıtılması ve anahtar yönetimi yaşam çevriminin sona ermesi aşamalarını kapsamaktadır.

4.2.2.2.1. ESHS anahtar çiftinin oluşturulması

Yönetmeliğin 18 inci maddesinin birinci fıkrasına göre ESHS'nin anahtar çifti ile elektronik sertifikasının Türkiye Cumhuriyeti sınırları içerisinde oluşturulması ve gizli anahtarın hiçbir şekilde bu sınırların dışına çıkarılmaması gerekmektedir.

Direktifin Ek–2 (g) bendi hükmü uyarınca ESHS'nin, kendi gizli anahtarını oluşturmasına ilişkin işlemleri gizlilik içinde yerine getirmesi gerekmektedir. Bu çerçevede ESHS, gizli anahtarını, gizlilik koşullarının sağlandığı ortamlarda oluşturmalıdır.

Gizli anahtarın oluşturulmasına ilişkin süreç, güvenilirliği kanıtlanmış en az iki personelin kontrolü altında ve fiziksel güvenliği sağlanmış bir ortamda yürütülmelidir. ESHS'nin önceden belirlemiş olduğu iş süreçlerine uygun olması gereken bu işlemlerin güvenli bir şekilde yürütülebilmesi için yetkilendirilen personelin asgari sayıda tutulması gerekmektedir [24].

ESHS'ye ait gizli anahtarı oluşturma işlemi için kullanılan güvenli elektronik imza oluşturma araçları; FIPS 140-2 (Federal Information Processing Standards Publications – Federal Bilgi İşleme Standartları Yayınları)'nin en az üçüncü seviyesinde belirlenen veya EAL 4 (Evaluation Assurance Level – Değerlendirme Garanti Düzeyi) ya da ISO/IEC 15408 standardının güvenlik seviyesine tekabül eden şartları karşılamalıdır.

ESHS'ye ait gizli anahtarın oluşturulmasına ilişkin işlemler; nitelikli elektronik sertifikaların kullanım amaçları ile paralellik arz eden bir algoritma ile

gerçekleştirilmelidir [101]. Bu nedenle, Tebliğin 6 ncı maddesi uyarınca, ESHS'ye ait gizli ve açık anahtarlara ilişkin algoritma ve parametrelerin;

- RSA için en az 2048 bit veya
- DSA için en az 2048 bit veya
- DSA Eliptik Eğrisi için en az 256 bit

olması gerekmektedir.

Yönetmeliğin 18 inci maddesinin ikinci fıkrasına göre ESHS'ye ait açık ve gizli anahtarların geçerlilik süresi en fazla on yıl olmalıdır. ESHS, anahtar çiftinin geçerlik süresinin bitiminden uygun bir süre önce, yeni anahtar çiftini oluşturmalı ve anahtarlarına güvenen kullanıcıların ve üçüncü kişilerin yapacakları işlemlerin devamı için gereken tüm tedbirleri almalıdır [101].

4.2.2.2.2. ESHS gizli anahtarının kullanılması, saklanması ve yedeklenmesi

ESHS, gizli anahtarını elektronik imza mevzuatında belirlenmiş kurallara ve ilgili uygulama dokümanlarına uygun bir şekilde kullanmalıdır. ESHS, elektronik sertifika oluşturma aşamasında kullanmış olduğu gizli anahtarı, sertifika iptal listelerini imzalamak için de kullanabilmektedir.

Yönetmeliğin 18 inci maddesinin birinci ve ikinci fıkraları uyarınca, ESHS'nin, kendi açık ve gizli anahtarları ile elektronik sertifikasını Türkiye Cumhuriyeti sınırları içerisinde oluşturması ve gizli anahtarını hiçbir şekilde bu sınırların dışına çıkarmaması gerekmektedir.

ESHS, gizli anahtarının gizliliğini ve bu anahtarın bütünlüğünün korunmasını temin etmelidir. ESHS'ye ait gizli anahtar, güvenilirliği kanıtlanmış en az iki personelin gözetiminde ve fiziksel açıdan güvenli bir ortamda saklanmalı ve yedeklenmelidir. Söz konusu hususların yürütülmesi için yetkilendirilecek personelin en az sayıda tutulması ve yapılacak işlemlerin ESHS'nin uygulama süreçlerine uygun olması

gerekmektedir. ESHS'ye ait gizli anahtarın yedek kopyaları, kullanılmakta olan anahtarın güvenlik seviyesine denk veya bu seviyeden daha üst düzeyde olmalıdır. Gizli anahtar; FIPS 140-2'nin en az üçüncü seviyesinde belirlenen veya EAL 4 ya da ISO/IEC 15408 standart serisinin güvenlik seviyesine tekabül eden şartları karşılayan güvenli bir kriptografik araçta tutulmalıdır.

ESHS'ye ait gizli anahtarın güvenliğinin tehlikeye düşmesi halinde ESHS; tüm kullanıcıları, sözleşme ilişkisi içinde bulunduğu kurumları ve diğer üçüncü kişileri bu durum hakkında bilgilendirmeli, ayrıca, bu gizli anahtarın kullanılması ile yayınlanan elektronik sertifikaların ve bu sertifikalara ait iptal durum bilgisinin artık geçerli olmayacağını belirtmelidir. Algoritmaların veya ilgili parametrelerin kullanım süresinin yetersiz kalması durumunda ESHS, tüm kullanıcıları, sözleşme ilişkisi içinde bulunduğu kurumları ve diğer üçüncü kişileri bu durum hakkında bilgilendirmeli ve bu durumdan etkilenmiş elektronik sertifikaları iptal etmelidir [26], [101].

4.2.2.2.3. ESHS açık anahtarının ve özetleme algoritmasının yayınlanması

Direktifin Ek 2 (f) ve (g) bentleri doğrultusunda ESHS'ye ait açık anahtarın üçüncü kişilerin erişimine açık tutulması gerekmektedir.

Yönetmeliğin 18 inci maddesinin üçüncü fıkrası uyarınca ESHS'nin, faaliyete geçmesini müteakip yedi gün içinde; sertifikasının sertifika özet değerini ve özetleme algoritmasını kendi internet sayfasında yayımlaması, ulusal yayın yapan en yüksek tirajlı üç gazetede ilan vermek suretiyle kamuoyuna duyurması ve gazete ilanlarının bir örneğini Kuruma iletmesi gerekmektedir.

4.2.2.2.4. ESHS anahtar yönetimi yaşam çevriminin sona ermesi

ESHS anahtar yönetimi yaşam çevrimi, anahtarların geçerlilik süresinin dolması gibi nedenlerle sona ermektedir. ESHS, anahtar yönetimi yaşam çevriminin sona

ermesinden sonra kendi gizli anahtarını kullanmamalıdır. Bu nedenle, ESHS'ye ait bütün gizli anahtarların kopyaları imha edilmeli veya kullanım dışı bırakılmalıdır.

4.2.3. Sertifika yönetimi yaşam çevrimi

Sertifika yönetimi yaşam çevrimi; elektronik sertifika için başvurulması, sertifikanın oluşturulması, yayınlanması, yenilenmesi, güncellenmesi, askıya alınması, iptal edilmesi ve sertifika kullanım dokümanlarının dağıtılması aşamalarına ilişkin hususları kapsamaktadır.

4.2.3.1. Sertifika başvurusu

Yönetmeliğin 9 uncu maddesine göre ESHS'nin, nitelikli elektronik sertifika vereceği kişilerin kimliğini; nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere göre tespit etmesi gerekmektedir. ESHS, nitelikli elektronik sertifika başvurusu sırasında sertifika verilecek kişiye ait kimliğin doğru ve güvenilir biçimde tespit edilmesinden sorumludur.

Her ne kadar sertifika verilecek kişinin kimlik tespiti esnasında bizzat hazır bulunması gerekse de, ESHS, nitelikli elektronik sertifika verilecek kişinin kimliğinin yukarıda belirtilen usuller ile önceden tespit edilmiş olduğu hallerde veya kurumsal başvurularda[14] kimlik tespiti için bizzat hazır bulunma şartını aramayabilmektedir. Kurumsal başvuru sahibinin, adına başvuruda bulunduğu kişilerin sertifika taleplerini yazılı olarak belgelendirmesi gerekmektedir.

Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisinin, mesleki veya diğer kişisel bilgilerinin sertifikada yer alması durumunda, ESHS, bu bilgileri resmi belgelere dayanarak eksiksiz, doğru ve güvenilir biçimde tespit etmelidir. ESHS, sertifika verilecek kişiden, sertifika vermek için gerekli olan bilgiler hariç bilgi talep

[14] Kurumsal başvuru, bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusunu ifade etmektedir.

etmemeli, bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletmemeli ve başka amaçlarla kullanmamalıdır.

Yönetmeliğin 15 inci maddesi doğrultusunda sertifika sahibi, elektronik sertifika almak için gerekli tüm bilgi ve belgeleri eksiksiz ve doğru olarak sağlamak ve ESHS'ye vermiş olduğu bilgilerde değişiklik meydana gelmesi halinde ESHS'yi derhal bilgilendirmek ile yükümlü kılınmıştır.

ESHS, Direktif Ek 2 (k) bendi hükmü gereğince, elektronik sertifika talep eden kişi ile hukuki bir ilişkiye girmeden önce ilgili kişiyi elektronik sertifikanın kullanımına ilişkin hususlar hakkında bilgilendirmeli ve bilgilendirme aşamasında kolayca anlaşılabilir bir dilin kullanılmasına özen göstermeli, ayrıca, sertifikanın kullanımına ilişkin bilgilendirme dokümanlarını kullanıcıların ve üçüncü kişilerin erişimine açık tutmalıdır.

Bununla bağlantılı olarak, Yönetmeliğin 14 üncü maddesinin birinci fıkrasında Direktif hükmüne paralel bir düzenleme yapılmış, bu çerçevede, ESHS'nin; elektronik sertifika verilecek kişiyi elektronik sertifika vermeden önce elektronik sertifikanın kullanımı ile ilgili usul ve sınırlamaların kapsamına ilişkin bilgilendirmesi gerektiği belirtilmiştir.

Söz konusu dokümanlarda; sertifikanın kullanım kısıtlarına, ESHS'nin ve kullanıcının yükümlülüklerine, üçüncü kişinin güveneceği sertifikanın iptal durumunun kontrol edilmesine ve sertifikanın doğrulanmasına, sertifika başvurusu sırasında alınan bilgilerin saklanma süresine ve uyuşmazlık çözüm süreçlerine ilişkin hususlara yer verilmesi gerekmektedir.

Yönetmeliğin 14 üncü maddesinin birinci fıkrası çerçevesinde ESHS, bilgilendirme yükümlülüğünü sertifika talep eden kişi ile sertifika sözleşmesi veya taahhütnamesi yaparak yerine getirmektedir. Söz konusu sözleşme veya taahhütname, güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğuna, sertifika talep eden kişinin

gizli anahtarını ve imza oluşturma aracını başkasına kullandırmamasına, elektronik sertifikanın iptal durumuna ve taraflar arasında çıkacak uyuşmazlıklarda başvurulabilecek alternatif uyuşmazlık çözüm yollarına ilişkin hususları kapsamalıdır. Ayrıca, nitelikli elektronik sertifikanın geçerlilik süresinin sözleşme veya taahhütname ile belirlenmesi gerekmektedir.

4.2.3.2. Sertifikanın oluşturulması, yayınlanması ve erişime açılması

ESHS, nitelikli elektronik sertifika başvurusunu müteakip, Tebliğ'in 5 inci maddesi gereğince sertifikayı ETSI TS 101 862 ve ITU-TRec. X.509V.3 standartlarına uygun olarak oluşturur, sertifika sahibine teslim eder ve kamuya açık bir dizinde[15] yayınlar.

Kanunun 9 uncu maddesi uyarınca nitelikli elektronik sertifikada;

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,
- ESHS'nin kimlik bilgileri ve kurulduğu ülke adının,
- İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,
- Gizli anahtara karşılık gelen açık anahtarın,
- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,
- Sertifikanın seri numarasının,
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,
- Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin,
- Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin,
- ESHS'nin sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının

bulunması zorunludur.

ESHS, kendi sertifikasyon alanı içinde bulunan kullanıcılara verilen isimlerin tekilliğini sağlamalı, diğer bir deyişle, ESHS tarafından yayınlanmış bir sertifikada kullanılan bir isim başka bir kişiye tahsis edilmemelidir [24].

---

[15] Dizin, geçerli sertifikaları içinde bulunduran elektronik depoyu ifade etmektedir.

Genel ilke olarak ESHS, elektronik sertifikaları, kullanıcıların ve üçüncü kişilerin erişimine açık tutmalıdır. Ancak ESHS tarafından, elektronik sertifikanın kamuya açık bir dizinde yayınlanması için sertifika sahibinin onayının alınması gerekmektedir. Dizin hizmetinin doğrulama sürecindeki rolünden dolayı, ESHS bu hizmeti kesintisiz olarak sağlamalıdır.

4.2.3.3. Sertifikanın yenilenmesi ve güncellenmesi

Yönetmeliğin 12 nci maddesinde nitelikli elektronik sertifikanın, geçerlilik süresinin sona ermesinden önce sertifika sahibinin veya sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda ESHS tarafından sertifika sahibine ait bilgilerin geçerliliği doğrulanarak yenilenebileceği hüküm altına alınmıştır.

ESHS, sertifika yenileme taleplerinin sertifika sahibi tarafından eksiksiz, doğru ve usulüne uygun bir şekilde yapılmasını temin etmelidir. Bu durum, sertifikanın geçerlilik süresinin tamamlanmasından önce veya iptal edilmesinden sonra yeniden anahtarlama işlemlerinin yapılmasını veya kişinin kimlik bilgilerinde değişiklik olması durumunda sertifikanın güncellenmesi durumunu da kapsamaktadır.

ESHS, sertifikanın yenilenmesi sırasında sertifikanın geçerliliğini, kimlik bilgilerinin doğruluğunu ve kullanıcıya ait kimlik bilgilerinin halen geçerli olup olmadığını kontrol etmelidir. Kişilere ait kimlik bilgilerinin değişmesi veya önceki sertifikanın iptal edilmesi durumunda, kimlik doğrulama bilgilerinin teyit edilmesi gerekmektedir [26].

ESHS, kullanıcıya ait gizli anahtarın üçüncü kişiler tarafından ele geçirilmemiş olması ve gizli anahtarın güvenliği noktasında yeni sertifika için gereken geçerlilik süresinin yeterli olması durumunda, kullanıcının önceki sertifikasında yer alan açık anahtarı kullanmak suretiyle yeni bir sertifika oluşturabilmektedir [101].

Yönetmeliğin 13 üncü maddesinin üçüncü fıkrası uyarınca; ESHS'nin gizli anahtarının çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması ya da sertifika ilkelerinin değişmesi gibi sertifika sahibinin kusurunun bulunmadığı durumların sonucunda, nitelikli elektronik sertifikaların ESHS tarafından iptal edilmesi ve yenilenmesi halinde, yenileme işlemleri için herhangi bir ücretin talep edilmemesi gerekmektedir.

4.2.3.4. Sertifikanın askıya alınması ve iptal edilmesi

Direktif Ek II (b) bendi hükmü gereğince ESHS, iptal taleplerine anında karşılık verebilecek güvenli dizin ve iptal hizmetini sağlamalı ve doğrulanmış sertifika iptal talepleri doğrultusunda kullanıcı sertifikalarını güncel olarak iptal etmelidir.

Kanunun 11 inci maddesi uyarınca ESHS; nitelikli elektronik sertifika sahibinin talebi, nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin, yanlışlığının ortaya çıkması, bilgilerin değişmesi, nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının ve iflasının veya gaipliğinin ya da ölümünün öğrenilmesi durumlarında vermiş olduğu nitelikli elektronik sertifikaları derhal iptal etmesi gerekmektedir.

Yönetmeliğin 13 üncü maddesinde ise; elektronik sertifikanın iptaline ilişkin taleplerin ESHS, sertifika sahibi ve sözleşme ile belirlenen kişiler tarafından yapılabileceği, ESHS'nin, bu duruma ilişkin taleplerin yapılabilmesini, asgari olarak telefonla ve kesintisiz sağlaması gerektiği hüküm altına alınmıştır.

İptal talebinin alınmasından sonra nitelikli elektronik sertifika derhal iptal edilmektedir [106][16]. İptal edilen nitelikli elektronik sertifika, geçerlilik süresi sonuna kadar iptal durum kayıtlarında[17] yer almaktadır. ESHS, nitelikli elektronik

[16] Yönetmeliğin 13 üncü maddesinin ikinci fıkrasında nitelikli elektronik sertifikanın geçmişe yönelik olarak iptal yasağı bulunmaktadır.

[17] İptal durum kaydı, 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 kaydı ifade etmektedir.

sertifikalara ilişkin iptal durum kaydını herhangi bir kimlik doğrulamasına gerek olmaksızın ücretsiz ve kesintisiz olarak kamu erişimine açık tutmaktadır. Kayıtların bir sonraki güncelleme zamanı söz konusu kayıtlarda açıkça gösterilmektedir.

ESHS, iptal durum bilgisini doğrulamak için gereken süreden daha fazla süre için sertifikayı askıda bırakmamalı ve sertifika sahibini iptal edilen veya askıya alınan sertifikanın değişen durum bilgisine ilişkin bilgilendirmelidir. İptal durum kaydının bütünlüğünün ve doğruluğunun korunması, bu hizmetlere herkes tarafından erişilebilmesi ve sertifikanın geçerlilik süresi sona erene kadar sertifika iptal durum bilgisinin sertifikanın durumuna ilişkin bilgileri içermesi gerekmektedir.

Nitelikli elektronik sertifikanın belirli bir süre kullanım dışı bırakılmak istenmesi veya anahtar çiftinin güvenliği ile ilgili şüpheye düşülmesi gibi sebeplerle sertifikanın askıya alınması talebi söz konusu olabilmektedir. Askıya alma, iptalden farklı olarak geriye dönülebilir bir işlemdir. İptal edilen sertifikalar yeniden geçerlilik kazanamazken, askıya alınmış sertifikalar askı durumundan çıkartılarak yeniden geçerlilik kazanabilmektedir. İptali talep edilmiş sertifikalar, iptal talebi sertifika sahibi tarafından onaylanıncaya kadar ESHS tarafından askıya alınmaktadır [26].

4.2.4. ESHS'nin güvenlik yaklaşımları

Kanunun 8 inci maddesi uyarınca ESHS; güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile yükümlü kılınmıştır. Güvenilir bir yapının varlığı, ancak ESHS'nin söz konusu yükümlülüklerini yerine getirmesi ile mümkün olabilmektedir.

Bu çerçevede; sertifika hizmetlerini herkese eşit bir şekilde sunması, yapının mer'i mevzuat hükümlerine uygun bir şekilde kurulmuş olması ve işleyişe ilişkin yükümlülükleri karşılayabilecek mali güce sahip olması ESHS'nin "güvenilir" olduğuna karine teşkil etmektedir. Ayrıca belirtmek gerekir ki, ESHS'nin sertifika

oluşturma ve iptal yönetimi ile ilgili birimlerinin diğer birimlerden bağımsız olması yapının güvenilirliği noktasında önemli bir diğer husus olarak nitelendirilmektedir [101].

ESHS'nin güvenlik yaklaşımları çerçevesinde; bilgi güvenliği yönetimi, varlık ve veri sınıflandırması, iletişim ve işletim güvenliği, sistem erişim güvenliği, iş süreklilik yönetimi, çalışanların güvenliği, fiziksel ve çevresel güvenlik ile elektronik sertifikalara ilişkin bilgilerin güvenliği hususları incelenecektir.

4.2.4.1. Bilgi güvenliği yönetimi

Bilgi güvenliği altyapısı, bilgi güvenliği ile ilgili yapılacak işlemleri işletme içinde başlatmak ve kontrol etmek amacıyla kurulan altyapıdır [1]. ESHS, *"kurumsal bilgi güvenliği"*ne ilişkin altyapıyı oluşturmalı ve sürekli işler halde bulundurmalıdır. Bu çerçevede ESHS yönetimi; bilgi güvenliğinin korunmasına ilişkin yükümlülüklerini tanımlamak ve bu yükümlülüklerini yerine getirmek suretiyle bilgi güvenliği altyapısını desteklemelidir. Bilgi güvenliğinin *"kurumsal"* nitelik taşıması, ESHS'nin bütün birimleri tarafından desteklenmesine bağlıdır. Bu nedenle, bilgi güvenliğine ilişkin faaliyetler, ESHS'nin değişik birimlerinde çalışan, farklı rolleri ve işlevleri üstlenmiş çalışanların işbirliği ile yürütülmelidir [103].

Bilgi güvenliği yönetiminin etkin bir şekilde işleyebilmesi için, ESHS'nin işleyişinde bazı rollerin belli kişilere tahsis edilmesi gerekmektedir. Örneğin; güvenlik süreçlerinin uygulanmasına ilişkin yönetimin sorumluluğunu taşıyan güvenlik memurları, sertifika oluşturma, iptal ve askı işlemlerini onaylamaktan sorumlu kayıt memurları, güvenli sistemlerin kurulması ve sürdürülmesi ile sorumlu sistem yöneticileri, güvenli sistemleri işletmekle ve sistem yedeklemesini yapmakla sorumlu olan sistem işletmecileri, istenildiğinde arşiv ve denetim kayıtlarını göstermekten sorumlu sistem denetçileri ESHS bünyesinde tanımlanması gereken roller olarak bilinmektedir [106].

ESHS'nin, güvenlik gereksinimlerini belirlemek ve sertifikasyon süreçleri için risk teşkil eden hususları tespit etmek üzere *risk değerlendirmesi* yapması gerekmektedir.[18] ESHS tarafından yapılacak risk değerlendirmeleri belli aralıklarla gözden geçirilmeli ve gereken hallerde revize edilmelidir [24].

Sertifikasyon hizmetlerinin görüldüğü ESHS'ye ait tesisler, bilgi varlıkları ve sistemler için operasyonel süreçlerin ve güvenlik denetimlerinin uygulanması ve bunların tevsik edilmesi gerekmektedir. Bilgi güvenliği yönetiminde ve uygulamasında takip edilen yaklaşımlar, güvenlik uygulamalarında önemli değişikliklerin ortaya çıkması durumunda, belli aralıklarla gözden geçirilmelidir.

Üçüncü kişilerin iş süreçlerinden kaynaklanan etkenlerin ESHS'ye ait verilere ve bilgi işlem araçlarının güvenliğine yönelik doğuracağı riskler tanımlanmalıdır. Farklı kurum veya kuruluşlar ile bilgi paylaşımı yapılması halinde ESHS'ye ait verilerin korunması için ESHS ile ilgili taraflar arasında gizlilik sözleşmesi yapılmalıdır. ESHS ile üçüncü kişiler arasında verilere ve bilgi işlem araçlarına erişim, bunların işlenmesi veya yönetilmesi ile ilgili yapılacak sözleşmelerde bilgi güvenliği şartları yer almalıdır [103].

Kanunun 12 nci maddesinde ESHS'nin elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemeyeceği ve bu bilgileri kişinin rızası dışında elde edemeyeceği, elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engellemesi gerektiği, bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemeyeceği ve başka amaçlarla kullanamayacağı hüküm altına alınmıştır. ESHS'nin; verilerin tahrip edilmesini veya kaybedilmesini önlemek amacıyla veri gizliliğine ve verilerin korunmasına ilişkin hükümleri eksiksiz bir şekilde uygulaması, bu kapsamda, kişisel verilerin tahrip edilmesine, kaybedilmesine veya

[18] İşletme içinde belirlenen ve envanteri tutulan varlıkların değerlerinin tespit edilmesini müteakip, bu varlıklara yönelik tehditlerin incelenmesi, söz konusu tehditlerin gerçekleşmesi durumunda ortaya çıkması muhtemel zayıflıkların belirlenmesi ve bu zayıflıklara karşı koruma tedbirlerinin alınması risk değerlendirmesinin ana başlıklarını teşkil etmektedir.

kanuna aykırı olarak işlenmesine karşı teknik ve hukuki tedbirler alması gerekmektedir.

İlgili düzenlemelerde yer alan hükümler çerçevesinde bilgi işlem araçlarının kullanıcılar tarafından hukuki olmayan amaçlar için kullanılmasının önüne geçilmeli, şifrelemeye ilişkin kontroller ilgili düzenlemelere uygun olarak kullanılmalı, ESHS'nin faaliyetlerine katılan yeni bilgi işlem araçları için idari yetkilendirme süreçleri tanımlanmalı ve uygulanmalıdır. Ayrıca, fikri mülkiyet hakkına tabi yazılım ürünlerinin kullanımına ilişkin yasal, idari veya akdi düzenlemelere uygun özel yöntemler kullanılmalıdır [101].

Bilgi güvenliğine ilişkin olayların, uygun idari süreçler marifetiyle hızlı bir şekilde raporlanmasının bilgi güvenliği açısından büyük önemi bulunmaktadır [103]. Zira bilgi güvenliğine ilişkin olaylara düzenli ve hızlı bir şekilde karşılık verilmesine olanak sağlayan raporlama sürecinin tesis edilmesi ve buna ilişkin yükümlülüklerin belirlenmesi ile sistemde tespit edilen güvenlik zaafları ortaya çıkarılmakta ve söz konusu zaafların giderilmesi mümkün olabilmektedir.

4.2.4.2. Verilerin ve varlıkların sınıflandırılması

ESHS'ye ait verilerin ve varlıkların[19] güvenliği açısından söz konusu unsurların sınıflandırılması büyük önem taşımaktadır. Bu çerçevede, varlıkların kullanımına ilişkin kurallar belirlenmeli, bu kurallar tevsik edilmeli ve uygulama aşamasına geçirilmelidir.

Bilgi varlıkları, yazılım varlıkları ve fiziksel varlıklar ESHS'nin başlıca varlıkları arasında yer almaktadır. Örneğin; veri tabanları ve veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri, süreklilik planları ve yedek anlaşmaları bilgi varlığı olarak kabul edilmektedir. Yazılım varlıkları arasında uygulama yazılımları, sistem yazılımları, geliştirme araçları, fiziksel varlıklar arasında bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler),

[19] ESHS için değeri olan herhangi bir şey varlık olarak tanımlanmaktadır.

manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri) bulunmaktadır [1].

ESHS'ye ait varlıklar kesin bir şekilde tespit edilmeli ve bütün önemli varlıkların envanteri hazırlanmalıdır. Bilgi işlem araçları ile ilgili varlıklar önceden belirlenmiş bir birime zimmetlenmelidir.

Belirli bir güvenlik seviyesinde korunması gereken veriler için *"Bilgi Sınıflandırma Şeması"*nın oluşturulması, sınıflandırmaya uygun olarak veri etiketleme ve veri işleme için gerekli süreçlerin tanımlanması gerekmektedir [103].

4.2.4.3. İletişim ve işletim güvenliği

İletişim ve işletim güvenliği ile

- Bilgi işlem araçlarının doğru ve güvenli bir şekilde işletilmesi,
- ESHS ile üçüncü kişiler arasında yapılan sözleşmelerin BGİ'ye uygun olması,
- Sistemin çökme ihtimaline ilişkin risklerin en aza indirilmesi,
- Yazılım ve veri bütünlüğünün korunması,
- ESHS'ye ait varlıklar üzerinde yetkisiz olarak yapılan değişikliklerin ve müdahalelerin önlenmesi,
- Taşınabilir medya[20] araçlarının korunması

amaçlanmaktadır [103].

ESHS tarafından; bilgi işlem araçları doğru ve güvenli bir şekilde işletilmeli, bu araçların işletimine ilişkin çalışma süreçleri belirlenmeli, söz konusu süreçler yazılı hale getirilmeli ve oluşturulan dokümanlar ilgili kişilerin erişimine açık tutulmalıdır.

ESHS ile çalışanlar veya üçüncü kişiler arasında tarafların yükümlülüklerinin açıkça tespit edildiği hizmet sözleşmesinin aktedilmesi gerekmektedir. ESHS ile üçüncü

[20] Taşınabilir medya araçlarına CD, disket ve USB aracı gibi donanımlar örnek olarak verilebilir.

kişiler arasında yapılan hizmet sözleşmelerinde; hizmet tanımlarına, hizmetlerin sağlanmasına ve güvenlik kontrollerine ilişkin hükümlere yer verilmelidir. Söz konusu sözleşmelerin ilgili hükümleri, BGİ süreçlerinde yapılacak değişiklikler çerçevesinde yeniden gözden geçirilmelidir. Üçüncü kişiler tarafından sağlanan hizmetler, tutulan kayıtlar ve hazırlanan raporlar düzenli bir şekilde izlenmeli ve değerlendirilmelidir [103].

ESHS'ye ait sistemin kapasite ihtiyaçları öngörülmeli, kaynakların kullanımı izlenmeli ve buna ilişkin gerekli düzenlemeler yapılmalıdır. Sistemin kabulünden önce ve gelişimi sırasında sistem için gerekli test çalışmalarının yürütülmesi, yeni sürümlerin, güncellemelerin ve kabul kıstaslarının tesis edilmesi gerekmektedir. ESHS; arızalarını en alt seviyeye indirerek güvenli bir şekilde sistemini işletmeli, sistem bütünlüğünü virüslere, kötücül ve izinsiz yazılımlara karşı korumalıdır [101].

ESHS, olaylara hızlıca cevap vermek ve güvenlik ihlallerinin olumsuz etkilerini sınırlandırmak için zamanında hareket etmelidir. Kötücül faaliyetleri belirlemek için sisteme ilişkin denetim kayıtları (logları) izlenmeli ve bu kayıtlar düzenli bir şekilde gözden geçirilmelidir. Güvenliği ihlal eden olay ve arızalar, söz konusu durumlara ilişkin raporlama yapılması ve cevap süreçlerinin belirlenmesi suretiyle asgari seviyeye düşürülmelidir.

Erişim kontrolünün izlenmesi amacıyla kullanıcı etkinliklerinin, kuraldışılıklarının ve bilgi güvenliği olaylarını içeren denetim kayıtlarının belirli bir süre için saklanması gerekmektedir. Sistem yöneticisi ve işletimcisinin faaliyetleri ile birlikte sistem hataları da kayıt altına alınmalıdır [26].

Yazılımları kötücül kodlara karşı korumak için tespit, engelleme ve kurtarma kontrollerinin yapılması gerekmektedir. Verilerin ve yazılımların yedekleri tutulmalı ve bu yedekler düzenli bir şekilde kontrol edilmelidir. ESHS'ye ait verileri yanlış kullanımdan korumak amacıyla söz konusu verilerin kullanılmasına ve depolanmasına ilişkin süreçler tesis edilmeli, sistem dokümantasyonu yetkisiz erişime karşı korunmalıdır. ESHS'ye ait varlıklar üzerinde yapılacak yetkisiz

değişikliklerin ve müdahalelerin önlenmesi amacıyla, çalışanların sorumluluk ve görev alanları birbirinden kesin çizgilerle ayrılmalıdır.

Taşınabilir medya araçlarının yönetimine ilişkin süreçler belirlenmeli, kullanılmayan medya araçları önceden tespit edilmiş yöntemler ile güvenli bir şekilde bertaraf edilmelidir. Veri taşıyan medya araçları, yetkisiz erişimden ve muhtemel suistimallerden korunmalıdır [101].

4.2.4.4. Sistem erişim güvenliği

Sistem erişim güvenliği ile

- Bilgi sistemlerine ve ağ hizmetlerine yetkisiz erişimin engellenmesi,
- Veri erişiminin kontrol edilmesi,
- Bilgi işlem araçlarının korunmasına yönelik tedbirlerin alınması

amaçlanmaktadır [103] .

ESHS tarafından; erişim kontrol ilkeleri oluşturulmalı ve bu ilkeler yazılı hale getirilmelidir. Söz konusu ilkeler çerçevesinde; bilgi sistemlerine ve ağ hizmetlerine erişilmesine ve erişimin iptal edilmesine ilişkin hususlar kayıt altına alınmalı, işlem imtiyazları sınırlandırılmalı ve bu işlemler kontrol edilmelidir. Sözü edilen hususların gerçekleştirilebilmesi için taşınabilir medya araçlarına ilişkin temiz masa ilkelerinin, bilgi işlem araçları için temiz ekran ilkelerinin uygulanması gerekmektedir.

Kullanıcıların güvenlik gereklerine uygun olarak seçmekle ve kullanmakla yükümlü olduğu erişim şifrelerinin, ESHS tarafından belirlenen idari süreçler doğrultusunda kullanıcılara dağıtılması ve kullanıcıların erişim haklarının düzenli aralıklarla gözden geçirilmesi temin edilmelidir. Ayrıca belirtmek gerekir ki, kullanıcılar sadece yetkili kılınmış oldukları hizmetlere erişim sağlayabilmeli, uzakta bulunan kullanıcıların erişimini kontrol etmek için kimlik doğrulama yöntemlerini kullanmalıdır. Özellikle

ESHS'nin faaliyet alanı dışında paylaşımlı ağları kullanan kullanıcıların söz konusu ağlara bağlanma yetkileri, erişim kontrol ilkelerine ve iş uygulamalarının gereklerine uygun olarak sınırlandırılmalıdır.

Sisteme erişim, *"güvenli oturum açma süreci"* ile kontrol edilmeli, erişim şifrelerinin yönetiminde uygulanan farklı sistemler karşılıklı biçimde etkileşim içinde olmalıdır. Belirli bir etkinsizlik periyodundan sonra etkin olmayan oturumlar kapatılmalı, yüksek risk taşıyan uygulamalarda ek güvenlik sağlamak için bağlantı süreleri üzerinde sınırlamaya gidilmelidir.

ESHS, sistem erişim kanallarını sadece usulüne uygun olarak yetkilendirilmiş kişilerin erişimine açmalıdır. İç ağ alanına üçüncü kişiler tarafından yapılacak sızmalara karşı söz konusu alanı korumak üzere ESHS tarafından güvenlik duvarı gibi bölümlerde periyodik kontrollerin uygulanması gerekmektedir.[21] Yetkisiz erişim sağlanması veya güvenli olmayan ağlar üzerinden veri değişimi yapılması gibi riskli durumlara karşı, "hassas nitelikteki veriler" şifreleme yöntemleri kullanılarak koruma altına alınmalıdır.[22]

ESHS; sistem güvenliğini idame etmek için işleticilerin, yöneticilerin ve sisteme doğrudan erişim hakkı bulunan kullanıcıların erişim kurallarını düzenlemelidir. ESHS; bilgi sistemlerine erişimin erişim kontrol ilkelerine uygun olarak sınırlandırıldığı ve SUE'de belirlenmiş güvenli rollerin ayırımı için yeterli güvenlik kontrollerinin yapıldığı bir sistemin altyapısını kurmalıdır. Özellikle yardımcı programların kullanımı sınırlandırılmalı ve bu durum sıkı bir şekilde kontrol edilmelidir. Kullanıcıya tanınmış rollerin yürütülmesi için gerekli olan kaynaklara erişim yetkisi dışında, kullanıcıların sisteme erişimi sınırlandırılmalıdır [103].

Sertifikasyon sürecine ilişkin uygulamalara geçilmeden önce bu uygulamaları yürütecek ESHS personeli belirlenmeli ve bu personelin kimlik doğrulaması

---

[21] Güvenlik duvarı, ESHS'nin operasyonları için gerekli olmayan erişimleri önlemek üzere yapılandırılmalıdır.

[22] Hassas veriler kayıt bilgilerini içermektedir.

yapılmalıdır. Söz konusu personel olay günlüklerinin tutulması gibi faaliyetlerinden dolayı sorumlu tutulmalıdır. Silinmiş dosyalara yetkisiz kullanıcılar tarafından erişilebilmesine karşı, hassas veriler koruma altına alınmalıdır [101].

Sistem kaynaklarına kural dışı ve yetkisiz erişim girişimlerini tespit etmek, kayıt altına almak ve bunlara cevap vermek için ESHS tarafından sürekli izleme ve alarm işlevleri uygulanmalıdır [106].

4.2.4.5. İş süreklilik yönetimi

Direktif Ek II (a) bendi hükmüne göre ESHS, sertifikasyon hizmetlerinin sağlanmasında *güvenilirlilik* unsurunu yerine getirmeli, bu çerçevede, gizli anahtarının güvenliğinin tehlikeye düşmesi durumu da dahil herhangi bir felaket durumunda faaliyetlerinin en kısa zamanda geri yüklemesini temin edecek *"iş sürekliliği yönetimini"* kurmalıdır.

İş süreklilik yönetimi ile ESHS'nin faaliyetlerine yönelik müdahelelerin etkisiz hale getirilmesi ve bilgi sistemlerinden kaynaklanan felaketlerden ve aksaklıklardan ESHS'nin korunması amaçlanmaktadır.

ESHS, herhangi bir felaket durumunda kullanmak üzere iş süreklilik planını belirlemeli ve bu planı uygulamalıdır. İş sürekliliği planlarının etkinliği açısından bu planların düzenli olarak uygulanması ve güncellenmesi büyük önem arz etmektedir. Söz konusu plan; iş akışında kesintilere yol açabilecek olaylar, bu olayların bilgi güvenliği noktasında doğuracağı sonuçlar ve bu sonuçların muhtemel etkileri dikkate alınarak tanımlanmalıdır.

İş süreklilik planlarına ilişkin şartların karşılanması açısından, hayati önemi haiz bilgilerin ve yazılımların yedekleme kopyaları düzenli bir şekilde tutulmalı, herhangi bir felaketin ardından hayati önemi haiz bilgileri ve yazılımları kurtaracak yeterli yedekleme olanakları sağlanmalı ve bireysel sistemler için kullanılan yedekleme sistemleri düzenli olarak test edilmelidir [101].

4.2.4.6. Güvenlik bağlamında çalışanların nitelikleri

Yönetmeliğin 19 uncu maddesinde *"ESHS özel hukuk tüzel kişisi ise, kurucu ortakları, tüzel kişiliği temsile yetkili yöneticileri ve istihdam ettiği veya ettirdiği personeli; gerçek kişi ise kendisi, temsile yetkili yöneticileri ve istihdam ettirdiği personeli taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya altı (6) aydan fazla hapis yahut basit veya nitelikli zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtekârlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş olmalıdır.*
ESHS; bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam eder veya ettirir. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış olmalıdır. ESHS organizasyon şemasında istihdam ettiği veya ettirdiği tüm personelinin görev tanımını ve dağılımını belirler." hükmü yer almaktadır.

Direktif Ek II (e) hükmü uyarınca ESHS, ilgili hizmetlerin ifasında gerekli uzmanlık bilgisi ile mesleki tecrübeyi haiz, elektronik imza teknolojisine vakıf olan kişileri istihdam etmekle yükümlüdür. Söz konusu hükümler çerçevesinde, ESHS, ilgili hizmetlerin yürütülmesinde gereken uzmanlık bilgisini, tecrübeyi ve nitelikleri haiz yeterli sayıda çalışanı istihdam etmelidir.

ESHS bünyesinde çalışmak üzere işe alınacak adaylara ilişkin incelemeler ilgili mevzuat hükümlerine, idari düzenlemelere, etik kurallarına ve iş gereklerine uygun olarak yürütülmelidir. ESHS'nin yürütmüş olduğu faaliyetlerin güvenliğinde önemli pay sahibi olan güvenilir roller herhangi bir tereddüte mahal vermeyecek şekilde açıkça tespit edilmelidir. ESHS'nin sürekli ve geçici çalışanlarının görev ayrımlarının yapılması ve iş tanımlarının belirlenmesi gerekmektedir.

ESHS yönetimi; idari süreçler çerçevesinde belirlenen güvenlik koşullarının çalışanlar ve üçüncü kişiler tarafından uygulanıp uygulanmadığını takip etmeli, bütün çalışanları kurumsal politika ve süreçlere ilişkin konularda düzenli eğitimlere tabi tutmalıdır [24].

İş değiştirmeye veya işten ayrılmaya ilişkin yükümlülükler hizmet sözleşmelerinde ihtilafa yer bırakmayacak şekilde tanımlanmalıdır. ESHS çalışanları, işten ayrılmalarını müteakip kendilerine tahsis edilmiş olan varlıkları teslim etmeli, işten ayrılma veya iş değiştirme hallerinde verilere ve bilgi işlem araçlarına erişim hakları sona erdirilmelidir [103].

4.2.4.7. Fiziksel ve çevresel güvenlik

Yönetmeliğin 19 uncu maddesinin üçüncü fıkrasında ESHS'nin; güvenli sistem ve cihazları kullanması, bu sistem ve cihazlar ile bunların bulunduğu bina veya alanı koruması gerektiği belirtilmiş, ESHS'nin fiziksel ve çevresel güvenliğine ilişkin genel bir çerçeve çizilmiştir.

ESHS tarafından fiziksel ve çevresel güvenliğin sağlanması;

- Güvenli sistem ve cihazların kullanılması ve
- Söz konusu sistem ve cihazlar ile sistem ve cihazların bulunduğu bina ve/veya alanın korunması

ile mümkün olmaktadır.

Bu çerçevede, fiziksel ve çevresel güvenlik ile ESHS'nin müştemilatına ve faaliyetlerine yönelik yetkisiz erişim ve müdahalelerin önlenmesi ile varlıklara zarar verilmesine ilişkin tedbirlerin alınması amaçlanmaktadır.

Yönetmeliğin 19 uncu maddesinin üçüncü fıkrası kapsamında faaliyetlerin ESHS tarafından güvenli bir şekilde yerine getirilmesi için, fiziksel ve çevresel güvenlik ilkelerinin hazırlanması gerekmektedir. Söz konusu ilkeler; fiziksel erişim kontrolü,

doğal afet koruması, yangın güvenlik etkenleri, elektrik ve telekomünikasyon altyapısına ilişkin arıza halleri gibi hususları kapsamalıdır. Bu ilkeler kapsamında, ESHS'nin faaliyetlerini desteklemek için kullanılan güvenli sistem ve cihazların korunması ile fiziksel ve çevresel güvenlik kontrollerinin gerçekleştirilmesine ilişkin hususlar yer almalıdır.

ESHS, kritik önemi haiz hizmetlere fiziksel erişimin kontrol altında tutulmasını ve varlıklara karşı muhtemel fiziksel risklerin asgari seviyeye düşürülmesini sağlamalıdır. Bu itibarla; yangın, sel, deprem gibi felaketlerden doğacak zararları önlemek amacıyla, fiziksel koruma tedbirleri öngörülmeli ve uygulanmalıdır. Fiziksel güvenliğin sağlanması gereken alanlara girecek kişilerin mutlaka yetkili bir çalışanın gözetimi altında bulunması gerekmektedir. Yükleme ve dağıtım alanları gibi kamuya açık olan yerler kontrol edilmeli ve yetkisiz erişimleri önlemek için bu yerler, bilgi işlem araçlarının bulunduğu alanlardan tecrit edilmelidir.

Sertifikaların oluşturulması, imza oluşturma araçlarının hazırlanması ve iptal yönetim hizmetlerinin sağlanması aşamalarında kullanılan cihazlara sadece usulüne uygun olarak yetkilendirilmiş çalışanların erişebilmesi sağlanmalı, söz konusu cihazlar yetkisiz erişime ilişkin risklerin en aza indirildiği, fiziksel olarak korunaklı bir ortamda işletilmelidir. Sertifikaların oluşturulduğu, imza oluşturma araçlarının hazırlandığı ve iptal yönetim hizmetlerinin sağlandığı alanın etrafında fiziksel engeller oluşturmak suretiyle söz konusu alan, fiziksel anlamda koruma altına alınmalıdır [101].

Ayrıca ESHS tarafından, veri kaynaklarının ve bilgi işlem araçlarının yer aldığı alanları korumak amacıyla içinde güvenlik duvarlarının, kart okuyuculu giriş kapılarının ve güvenlik görevlilerinin bulunduğu güvenlik çemberinin kurulması gerekmektedir. Bilgi kaynaklarını ve bilgi varlıklarını korumak ve bu çerçevede sadece yetkili çalışanların erişimini temin etmek üzere, ESHS faaliyet alanının giriş noktalarında kimlik doğrulama işlemlerinin yapılması gerekmektedir [103].

ESHS'ye ait gerek teçhizatın, gerek verilerin gerekse de yazılımların ESHS'nin faaliyet sınırlarının dışına çıkarılmasının gerekmesi halinde, bu işler önceden yetkilendirilmiş kişiler tarafından gerçekleştirilmelidir.

ESHS'nin faaliyetlerinde kullanılan teçhizat, çevresel tehdit ve tehlikelerden kaynaklanan riskler dikkate alınacak şekilde konumlandırılmalıdır. Teçhizatın bütünlüğünü ve kullanılabilirliğini teminen periyodik bakım çalışmalarının yapılması gerekmektedir. Veri taşıyan veya veri hizmetlerini destekleyen iletişim kabloları da yetkisi olmayan kişilerin müdahalelerinden korunmalıdır [103].

4.2.4.8. Elektronik sertifikalara ilişkin bilgilerin ve kayıtların güvenliği

Yönetmeliğin 14 üncü maddesinin ikinci fıkrası doğrultusunda ESHS;

- geçerlilik süresi sona eren nitelikli elektronik sertifikaları,
- nitelikli elektronik sertifika başvurusunda talep edilen bilgi, belge ve elektronik verileri,
- Sİ, SUE, ZDİ (Zaman Damgası İlkeleri ve ZDUE (Zaman Damgası Uygulama Esasları) dokümanlarını,
- geçerlilik süresinin sona ermesinden itibaren kendi sertifikasını,
- nitelikli elektronik sertifika yönetimine ilişkin tüm işlemlere, bu işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kaydı en

az yirmi yıl süreyle saklamakla yükümlü kılınmıştır.

ESHS, söz konusu hüküm çerçevesinde, yukarıda belirtilen kayıtların bütünlüğünü ve gizliliğini sağlamalı ve söz konusu kayıtları Sİ'ye ve SUE'ye uygun olarak arşivlemelidir. Kanuni kovuşturma aşamasında delillere ulaşılması gerektiğinde sertifika ile ilgili kayıtların kullanılabilir durumda tutulması, diğer bir ifade ile kanuni kovuşturma aşamasında delillere ulaşılabilmesi için sertifikalar ile ilgili tüm bilgilerin uygun bir süre için kayıt altına alınıp saklanması gerekmektedir [106].[23]

[23] Söz konusu kayıtlar sertifika ve anahtar yönetim olaylarına ilişkin bilgileri ve kayıt bilgilerini içermektedir.

Ayrıca, anahtar ve sertifika yönetimi olaylarına ilişkin kayıtlara ait kesin zaman bilgisinin de kayıt altına alınması gerekmektedir. Sertifikaların yenilenmesine veya yayınlanmasına ilişkin talepler de dahil olmak üzere tüm taleplere ilişkin olay günlükleri saklanmalıdır.

Erişim kontrolünün izlenmesi amacıyla kullanıcı etkinliklerinin, kuraldışılıklarının ve bilgi güvenliği olaylarını içeren denetim kayıtlarının da belirli bir süre için saklanması gerekir. Sistem yönetici ve sistem işlemci etkinlikleri ile sistem hatalarına ilişkin kayıtlar tutulmalı ve analiz edilmelidir. Tutulan kayıtlara ilişkin veriler tahrifata ve yetkisiz erişime karşı koruma altına alınmalıdır.

Ayrıca, sertifikaların ve ESHS anahtarlarının yaşam döngüsü ile iptale ilişkin tüm taleplerin ve olay bilgilerinin silinmeyecek veya tahrif edilmeyecek şekilde kayıt altına alınması gerekmektedir [103].

4.2.5. Zaman damgası ve hizmetleri

Yönetmeliğin 31 inci maddesi gereği ESHS'nin, Kanun kapsamında zaman damgası yayınlaması ve zaman damgası yönetimi ve operasyonları ile ilgili hizmet vermesi gerekmektedir. Bu çerçevede ESHS, ZDİ ve ZDUE dokümanlarını ETSI TS 102 023'e uygun olarak hazırlamalıdır.

ESHS'nin, zaman damgası üretilmesi işlemine ilişkin genel kuralları ortaya koyan ZDUE ve ZDİ dokümanlarını hazırlaması gerekmektedir. Bu dokümanlar, bu sürecin katılımcılarını tanımlamakta, sorumluluklarını, haklarını ve uygulanabilirlik aralığını belirtmektedir. ZDUE ve ZDİ dokümanlarının tüm kullanıcıların ve üçüncü kişilerin erişimine açık olması gerekmektedir.

ESHS Zaman Damgası Sağlayıcı, elektronik ortamda gerçekleştirilen bir işlem için zaman bilgisi oluşturan zaman damgası hizmetlerini ESHS bünyesinde sağlama noktasında işlev gören güvenilir bir birimdir. Zaman damgası hizmeti ile veri

değerlerini şifreleme yöntemiyle zaman değerlerine bağlayan zaman damgası işlemi yapılmaktadır.

Zaman damgası hizmetinin sağlanmasında bazı bileşenlerin önemli rolü bulunmaktadır. Söz konusu bileşenler kapsamında, zaman damgası talebinin doğruluğu ve bütünlüğü kontrol edilmekte, kesin zaman parametrelerini sağlayan güvenilir bir zaman kaynağı kullanılmakta, mevcut zaman bilgisini zaman damgası gerektiren veri ile bağlayan bir zaman damgası oluşturulmakta ve söz konusu zaman damgası bilgisi talepte bulunan imza sahibine iletilmektedir [106].

Tebliğin 10 uncu maddesi uyarınca ESHS'nin, zaman damgası ve hizmetlerine ilişkin olarak CWA 14167–1 ve ETSI TS 101 861 standartlarına uyması gerekmektedir. Bu kapsamda, ESHS, önceden takvime bağlanmış ve ayrı dokümanlarda belirtilmiş donanım ve sistem bakımıyla ilgili teknik atalet zamanları dışında zaman damgası hizmetlerine sürekli erişimi temin etmelidir. Zaman damgası içine yerleştirilen UTC zamanı en az ±100 ms doğruluk oranını sağlamalıdır.

ESHS tarafından çıkarılan her zaman damgası gerçek UTC zaman değerine kadar geriye doğru izlenebilecek tarih ve zaman değerini içermelidir. Temel saat, GPS (Global Positioning System – Küresel Konum Bulma Sistemi) uydu alıcısı ve atomik saati ile sunulmalıdır. ESHS'nin, uydu saatinin arızalanması durumunda ikincil saatlere sahip olması gerekmektedir. Saatin ölçümlemesinin bozulması, saatle oynanması ya da saatin fiziksel zarar görmesini engellemek için ESHS'nin yetkisiz kullanımı önleyecek güvenlik kontrollerini uygulaması gerekmektedir [18].

4.2.6. Faaliyetin sona ermesi

Kanunun 11 inci, Yönetmeliğin 29 uncu ve 30 uncu maddeleri uyarınca ESHS'nin faaliyetleri iki şekilde sona ermektedir:

- Kurum tarafından faaliyete son verilmesi,
- ESHS'nin kendi faaliyetine son vermesi.

4.2.6.1. Kurum tarafından faaliyete son verilmesi

Yönetmeliğin 29 uncu maddesi uyarınca Kurum, ESHS'nin faaliyetinin devamı sırasında bildirim şartlarından[24] birini veya birkaçını kaybettiğini tespit etmesi halinde ESHS'ye bu eksikliğin giderilmesi için bir aya kadar süre vermekte ve bu süre içinde ESHS'nin faaliyetlerini durdurmaktadır. Kurum,

- Verilen sürenin sonunda eksikliğin giderilmemesi veya
- Kanunun 18 inci maddesindeki suçların işlendiği tarihten itibaren geriye doğru üç yıl içinde üçüncü kez işlenmiş olması

hallerinde ESHS'nin faaliyetine son vermektedir.

Yukarıda belirtilen faaliyete son verme hallerinden birinin gerçekleşmesi ile faaliyetine son verilen ESHS, faaliyete son verme kararının tebliği tarihinden itibaren onbeş gün içinde faaliyette bulunan herhangi bir ESHS ile sertifikaların devri konusunda anlaşabilmektedir. Kurum, taraflar arasında anlaşma sağlanması durumunda, faaliyetine son verilen ESHS'nin oluşturduğu sertifikaların anlaşma sağlanan ESHS'ye devredilmesine karar vermektedir. Faaliyetine son verilen ESHS ile faaliyette bulunan herhangi bir ESHS arasında onbeş gün içinde devre ilişkin anlaşma sağlanamaması durumunda Kurum, sertifikaların herhangi bir ESHS'ye devrine re'sen karar verebilmektedir. Bu çerçevede, sertifikaları devralan ESHS sertifika yenileme işlemlerini başlatmakta ve devir kararının tebliği tarihinden itibaren bir ay içinde bu işlemleri tamamlamaktadır.

Kurumun faaliyete son verme kararının tebliğinden itibaren ESHS'nin elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlaması

---

[24] Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini içeren dilekçeyi ve bildirim şartlarını eksiksiz olarak Kuruma ibraz etmek suretiyle bildirimde bulunur. Söz konusu bildirim şartları arasında; ESHS'nin iletişim bilgileri, şirket ile ilgili belgeler, personel nitelikleri, Sİ, SUE, ZDİ, ZDUE, kendi sertifikasının örneği, sertifika mali sorumluluk sigortası, sözleşme ve/veya taahhütnameler örneği ve yapılan hizmet sözleşmesi örnekleri yer almaktadır.

sınırlandırılmakla beraber, sertifika yenileme işlemleri tamamlanıncaya kadar iptal durum kaydı hizmetini devam ettirebilmektedir.

Faaliyetine son verilen ESHS, sertifikaları devralan ESHS'ye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devretmesi ve kendi gizli anahtarı ile yedeklerini imha etmesi gerekmektedir.

Kurum, sertifikaları re'sen devredebileceği herhangi bir ESHS'nin bulunmaması durumunda, faaliyetine son verdiği ESHS'nin oluşturduğu sertifikaların iptal edilmesine karar verebilmektedir. Faaliyetine son verilen ESHS'nin son iptal durum kaydını oluşturduktan sonra kendi gizli anahtarı ile yedeklerini imha etmesi, geçerlilik süresi en geç sona eren sertifikanın geçerlilik süresi sonuna kadar iptal durum kaydı hizmetini devam ettirmesi ve arşivi en az yirmi yıl süreyle saklaması gerekmektedir.

Faaliyetine son verilen ESHS'nin, devredilmesine ilişkin kararları sertifika sahiplerine elektronik posta ile duyurması ve internet sayfasında yayımlaması gerekmektedir.

4.2.6.2. ESHS'nin kendi faaliyetine son vermesi

Yönetmeliğin 30 uncu maddesi uyarınca ESHS'nin, faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma yazılı olarak bildirmesi gerekmektedir. ESHS, faaliyetine son verme kararının Kuruma bildirilmesinden itibaren sertifika başvurusu kabul edememekte ve yeni nitelikli elektronik sertifika oluşturamamaktadır.

ESHS faaliyetine son vereceği tarihten en az üç ay önce faaliyetine son verme kararını internet sayfasında yayımlar, sertifika sahiplerine elektronik posta ile bildirir ve ulusal yayın yapan en yüksek tirajlı üç gazetede ilan vermek suretiyle kamuoyuna duyurmaktadır.

ESHS; faaliyetine son verme tarihine kadar geçerlilik süresi sona ermeyecek ve kullanımı faaliyette bulunan herhangi bir ESHS tarafından sağlanabilecek sertifikaları, faaliyete son verme tarihinden bir ay öncesine kadar faaliyette bulunan herhangi bir ESHS'ye devredebilir. Faaliyetine son veren ESHS devir hususunda sertifika sahiplerini elektronik posta ile bilgilendirir. Sertifikaların devredilmesi halinde sertifikaları devralan ESHS, sertifika yenileme işlemlerini başlatır ve bir ay içinde bu işlemleri tamamlar. Kurum, uygun görmesi halinde, bir ayı geçmemek üzere ek süre verebilmektedir.

Sertifikaları devreden ESHS sertifikaları devralan ESHS'ye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devretmesi ve kendi gizli anahtarı ile yedeklerini imha etmesi gerekmektedir.

Faaliyetine son verme tarihinden bir ay öncesine kadar sertifikaların devredilememesi veya sertifikaların kullanımının faaliyette bulunan herhangi bir ESHS tarafından sağlanamaması durumunda, faaliyetine son vermek isteyen ESHS, sertifikaları, faaliyete son verme tarihinde iptal eder. Faaliyetine son veren ESHS son iptal durum kaydını oluşturduktan sonra kendi gizli anahtarı ile yedeklerini imha eder [101], geçerlilik süresi en geç sona eren sertifikanın, geçerlilik süresi sonuna kadar iptal durum kaydı hizmetini devam ettirmesi ve arşivi en az yirmi yıl süreyle saklaması gerekmektedir.

5. ESHS'LERİN DENETİMİNE İLİŞKİN SONUÇ VE ÖNERİLER

Önceki bölümlerde, ESHS'lerin denetimi ile ilgili bilgilere ve değerlendirmelere yer verilmiştir. Bu bölümde, söz konusu bilgiler ve değerlendirmeler çerçevesinde ülkemizde faaliyet gösteren ESHS'lerin etkin ve verimli bir şekilde denetlenmesi kapsamında; Denetim Rehberinin hazırlanmasına ve uygulanmasına ilişkin önerinin yanında, kamu sektörüne sertifika hizmeti sağlayan kuruluşlara ilişkin denetim muafiyetinin sınırlandırılması, ihtiyari akreditasyon konusunun elektronik imza mevzuatı çerçevesinde düzenlenmesi, denetim usullerine ilişkin mevzuatın geliştirilmesi ve denetimlerin periyodik olarak uygulanması konularında değerlendirmeler yapılacak ve öneriler sunulacaktır.

- **Denetim Rehberinin Hazırlanması ve Uygulanması**

Sistematik bir süreç olan denetim çalışmalarının etkin bir şekilde yürütülmesi, sağlam bir hukuki altyapının kurulmasına bağlıdır. Bu altyapı, tarafların yetki ve yükümlülüklerine ve denetim sürecine ilişkin hususların denetim mevzuatı çerçevesinde düzenlenmesini gerekli kılmaktadır. Söz konusu düzenlemeler, denetim çalışmalarının usul ve esaslarına ilişkin hususları belirlemelidir.

Kurulduğu tarihten bu yana, kanun koyucu tarafından birçok alanda denetim yetkisi verilen TK açısından, denetim çalışmalarının usul ve esaslarını düzenleyen denetim mevzuatının hazırlanması, söz konusu yetkinin etkin ve verimli bir şekilde yerine getirilmesi bakımından büyük önem taşımaktadır. Mevcut durum dikkate alındığında, denetim düzenlemeleri noktasında birtakım eksikliklerin olduğu ve denetim mevzuatının oluşturulması ile bu eksikliklerin giderilmesi gerektiği değerlendirilmektedir. Bu çerçevede, ESHS'lerin denetimi dahil TK'nın tüm görev alanları ile ilgili hususları genel anlamda kapsayacak "Denetim Yönetmeliği"nin ve yönetmeliğin uygulanma biçimini gösterecek "Denetim Yönergesi"nin düzenlenmesi gerekmektedir. Nitekim TK bünyesinde söz konusu düzenlemelere ilişkin çalışmalara halen devam edilmektedir.

Ancak, söz konusu düzenlemeler genel anlamda denetim usul ve esaslarını belirlese de, denetim çalışmaları için sadece bu düzenlemelerin yeterli olmayacağı, TK tarafından denetim mevzuatının bir parçası olarak denetim rehberinin hazırlanmasının ve uygulanmasının gerekli olduğu değerlendirilmektedir.

Üçüncü bölümde açıklanan Güney Kore örneğinde görüldüğü üzere, KISA tarafından gerçekleştirilen denetimler, KCAC tarafından hazırlanan "Sertifika Hizmet Sağlayıcıları İçin Koruyucu Kurallar" ve denetim kapsamında yer alan hususları ve bu hususların hukuki dayanağını gösteren "Denetim Rehberi" dokümanları çerçevesinde yürütülmektedir. Zira denetim çalışmalarının yürütülmesi aşamasında, denetlenecek hususların somut olarak belirtildiği bir doküman niteliğinde olan denetim rehberi ile planlı bir denetimin gerçekleştirilmesi ve bu plan çerçevesinde denetlenecek hususların önceden tespit edilmesi mümkün olabilmektedir. Denetim rehberi, sistematik bir denetim çalışmasının önünü açması ve denetim çalışmalarının sağlıklı, etkin ve verimli sonuçlar doğurması bakımından oldukça önemli bir denetim aracıdır. Ayrıca, denetim rehberi denetim sırasında herhangi bir hususun gözden kaçmamasını sağlamakta ve kıstaslar ayrıntılı olarak belirtildiği için subjektifliği de asgari düzeye indirmektedir.

Kanunun 8 inci maddesi uyarınca ESHS; güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü hukuki ve teknik tedbiri almak ile yükümlü kılınmıştır. Söz konusu madde hükmü kapsamında alınması gereken tedbirlerin, elektronik imza mevzuatı kapsamında ESHS tarafından yerine getirilip getirilmediğinin kontrol edilebilmesi amacıyla Ek'te yer alan "Denetim Rehberi" hazırlanmıştır. Denetim rehberi, Kanunda, Yönetmelikte ve Tebliğde düzenlenen ve ESHS'nin uymakla yükümlü olduğu hususları kapsamaktadır. Bununla birlikte, Tebliğ ile atıf yapılan standartlar da denetim rehberinin kapsam alanı içinde bulunmaktadır.

Ayrıca, AAA'nın değişken özelliği ve elektronik imza uygulamalarının farklılığı nedeniyle denetime konu olan hususların zamanla değişebileceği yadsınamaz bir gerçektir. Bu nedenle değişen şartlara uygun olarak denetim rehberinin gözden

geçirilmesinin ve revize edilmesinin denetim çalışmalarının güncelliği bakımından ayrıca önemli olduğu değerlendirilmektedir. Bu itibarla, gereken hallerde, uygulamada denetim konusu olma özelliğini yitirmiş olan hususların çıkarılması veya gerekli görülen hususların ikame edilmesi suretiyle denetim rehberinin güncellenmesi gerektiği mütalaa edilmektedir.

- **Sertifika Hizmeti Sağlayan Kamu Kurum ve Kuruluşlarına İlişkin Denetim Muafiyetinin Sınırlandırılması**

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

8 inci maddenin dördüncü ve beşinci fıkraları uyarınca, faaliyetlerinin devamı sırasında ESHS'lerin, söz konusu maddede gösterilen şartları kaybetmeleri halinde TK tarafından faaliyetlerinin belli bir süre için durdurulacağı, söz konusu süre içinde bu şartları yerine getirmediklerinin tespiti halinde faaliyetlerine son verileceği ve ESHS'lerin TK'nın belirleyeceği ücret alt ve üst sınırlarına uymak zorunda olduğu belirtilmektedir. 15 inci maddede TK'nın denetim yetkisi, 19 uncu maddede ise 18 inci maddedeki suçları işleyen ESHS'lerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri halinde para cezalarının iki kat olarak uygulanacağı, üçüncü kez işlemeleri halinde ise TK tarafından ESHS'ler hakkında kapatma cezasının verileceği düzenlenmiştir.

Kanunun 21 inci maddesi çerçevesinde elektronik sertifika hizmeti sağlayan kamu kurum ve kuruluşları, TK'nın denetim kapsamı dışında tutulmuştur. Bu nedenle, TK denetimi dışında olan kamu kurum ve kuruluşlarının gerekli güvenlik şartlarını sağlayamaması veya sağlaması halinde söz konusu şartları sürdürememesi durumlarında [107], söz konusu uygunsuzluklar tespit edilememektedir.

Elektronik imza mevzuatının yürürlüğe girmesiyle birlikte giderek yaygınlaşan elektronik imza uygulamaları kapsamında; kamu kurum ve kuruluşlarının elektronik

ortamda yürütecekleri iş ve işlemlerde uyumlu, birlikte işler ve güvenilir bir yapıda çalışmalarını sağlamak maksadıyla, 10 Haziran 2004 tarihinde yapılan e-Dönüşüm Türkiye İcra Kurulu VI. Toplantısı'nda alınan 6 sayılı İcra Kurulu Kararı ile kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması kararlaştırılmış, bu kapsamda, tüm kamu kurum ve kuruluşlarının, kurumsal sertifika ihtiyaçlarının karşılanması amacıyla bir Kamu Sertifikasyon Yapısının oluşturulmasına karar verilmiştir. Bu çerçevede; tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifika yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulmasını ve sertifika yaşam çevriminin yönetilmesini sağlayacak Kamu Sertifikasyon Yapısının kurulması ve işletilmesi görev ve sorumluluğu TÜBİTAK – UEKAE'ye verilmiştir.

2004/21 sayılı Başbakanlık Genelgesi çerçevesinde, Kanunun 21 inci maddesi ile TK'nın denetim kapsamının dışında kalan UEKAE Kamu Sertifikasyon Yapısının *gözden geçirilmesi ve uygunluğunun izlenmesi* görev ve sorumluluğu TK'ya verilmiştir.

Ancak, Başbakanlık Genelgesi ile söz konusu yapının gözden geçirilmesine ve izlenmesine ilişkin TK'ya verilen yetkinin Kamu Sertifikasyon Yapısının uygunsuzluklarını tespit etme noktasında işlevsel olmadığı değerlendirilmektedir. Zira hukuki açıdan kanunkoyucunun denetim yetkisi tanımadığı bir alanda Başbakanlık Genelgesi ile denetim benzeri bir yetkinin kullanılmasının uygulamada birtakım sorunları beraberinde getirdiği gözlenmektedir.

Ayrıca, 21 inci madde ile getirilen muafiyetin Direktife aykırı olduğu da değerlendirilmektedir. Zira Direktifte SHS olarak faaliyet gösteren kamu kurum ve kuruluşlarının rekabete aykırı davranmamaları ve tekel oluşturmamaları gerektiği ifade edilmektedir. Kamu kurum ve kuruluşlarına bu konuda getirilecek muafiyetin tarafsız, şeffaf, ölçülü ve ayrımcılık oluşturmayacak bir niteliğe sahip olması, ayrıca bu muafiyetin ancak özel nitelikteki hususlar için tanınması gerekmektedir. Bu nedenle, Kanunun 21 inci maddesi ile kamu kurum ve kuruluşları lehine tanınan bu

muafiyetin, yukarıda belirtilen prensiplere aykırılık teşkil ettiği değerlendirilmektedir.

Bu itibarla, Kanunun 21 inci maddesinin sadece yukarıda sayılan durumlarda ve milli güvenlikle ilgili işlemlerde bulunan sınırlı sayıda kamu kurum ve kuruluşları bakımından muafiyet tanınarak değiştirilmesi gerektiği mütalaa edilmektedir.

- **İhtiyari Akreditasyon Konusunun Düzenlenmesi**

Üçüncü bölümde birbirinden farklı denetim yapılarına sahip olan Almanya ve Hollanda örnekleri incelenmiş, söz konusu ülkelerin aynı Direktife tabi olmalarına rağmen, birbirinden farklı denetim işlevlerine sahip oldukları tespit edilmiştir.

Alman mevzuatında sertifikasyon kuruluşlarına yer verilmiş olup, söz konusu kuruluşlar BNetzA tarafından yetkilendirilmektedir. Ayrıca BNetzA'nın SHS'ler üzerinde ihtiyari akreditasyon yetkisi bulunmaktadır. Hollanda mevzuatında da sertifikasyon kuruluşları düzenlenmiş, ancak söz konusu kuruluşlar akreditasyon kuruluşu olan RvA tarafından akredite edilmektedir. İlgili mevzuatta SHS'lerin akreditasyonu sertifikasyon kuruluşları tarafından yapılmakta, bu akreditasyon ise ihtiyari olmaktan çok, zorunlu bir nitelik arz etmektedir.

Türkiye'de ise Kanunun ilgili hükümleri uyarınca TK'nın ESHS'ler üzerinde sadece düzenleme ve denetim yapma yetkisi bulunmaktadır. Almanya ve Hollanda örneklerinin aksine, elektronik imza mevzuatında sertifikasyon işlevi dolaylı olarak belirtilmiş, akreditasyon kavramına ise yer verilmemiştir.

Güvenli elektronik imza oluşturma araçlarının sertifikasyonu için Tebliğin 11 inci maddesinin (b) bendinde; ESHS'nin, söz konusu araçların FIPS PUB 140–1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya CWA 14167-2'de belirtilen ölçütlere uygunluğunu veya CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu *yetkili kurum veya kuruluşlardan* alınan belgelerle

belgelendirmesi gerektiği hüküm altına alınmıştır. Söz konusu maddede belirtilen yetkili kurum veya kuruluşlar ifadesinden Direktifin 3.4 maddesinde de öngörülen sertifikasyon kuruluşlarının anlaşılması gerektiği düşünülmektedir. Bu itibarla, ulusal mevzuata göre, Türkiye'de veya yabancı ülkelerde yetkilendirilmiş ilgili kurum veya kuruluşlar sertifikasyon kuruluşu olarak kabul edilmektedir.

Bu tez kapsamında hazırlanan Denetim Rehberi çalışmasından çıkan sonuca göre ESHS'lerin denetiminde birçok teknik hususun denetlenmesi gerektiği tespit edilmiştir. Söz konusu teknik ayrıntıların dikkate alınmasını ve üst seviyede teknik bilgiyi gerektiren denetim çalışmaları kapsamında, ESHS'lerin mevzuatta atıf yapılan standartlara göre akredite olması denetçilerin iş yükünü de önemli ölçüde azaltacağı mütalaa edilmektedir. Ayrıca, TK'nın tanıyacağı akreditasyon kuruluşları tarafından akredite edilen herhangi bir ESHS'nin, teknik ve idari anlamda elde edeceği güvenilirlik niteliğinin ESHS'ler arasında hizmet kalitesi noktasında rekabetin yaşanmasına ve bu durumun elektronik imzanın kullanımının daha güvenli bir ortamda gerçekleştirilmesine imkân vereceği değerlendirilmektedir.

Bu itibarla, söz konusu denetim çalışmalarının etkin ve verimli bir şekilde yürütülebilmesi ve denetlenecek hususların azaltılması bakımından ESHS'lerin ETSI TS 101 456 standardı çerçevesinde akredite olmasına imkân veren ihtiyari akreditasyon müessesesine ilişkin düzenlemelerin yapılması gerekmektedir.

Bu çerçevede, 5070 sayılı Elektronik İmza Kanununa *"ESHS, başvuru üzerine, Kurumca tanınan yetkili akreditasyon kuruluşları tarafından akredite edilebilir. Yetkili akreditasyon kuruluşu tarafından akredite edilen ESHS'ye akreditasyon belgesi verilir. Yetkili akreditasyon kuruluşlarının tanınması ve ihtiyari akreditasyon hususlarına ilişkin düzenlemeler Kurum tarafından yapılır."*maddesinin eklenmesi, ayrıca, TÜRKAK (Türk Akreditasyon Kurumu) ve TSE (Türk Standartları Enstitüsü) ile koordineli çalışmaların yürütülmesi ve söz konusu kuruluşların bu konudaki bilgi birikiminden faydalanılması gerektiği değerlendirilmektedir.

- **Denetim Usullerine İlişkin Mevzuatta Yer Alan Hususların Geliştirilmesi**

Devlet faaliyetlerinin belirliliği ilkesi gereğince, idarenin davranışlarının belli ölçüde belirli, yani idare edilenlerce önceden görülebilir olması gerekmektedir. İdare, kanunların kendisine belli bir serbesti tanıyarak takdir yetkisi vermesi durumlarında da tamamen serbest hareket etme imkânına sahip değildir. Tam tersine, idare belli bir serbestîye sahip olduğu konularda da, bu konuları yönetmelik, tebliğ gibi idari metinlerle objektif bir biçimde düzenlemek veya sürekli uygulamaları ile hukuki istikrarı tesis etmek ve buna uymak zorundadır [108].

Devlet faaliyetlerinin belirliliği ilkesi doğrultusunda, ESHS'lerin denetiminde uygulanacak ilkelerin ve süreçlerin öngörülebilir olması gerekmektedir. Denetim çalışmalarına katılan ilgili taraflar için yol gösterici bir nitelik taşıyan denetim ilkelerinin, ilgili tarafların denetim işlevlerinin, planlama, inceleme, ön araştırma, soruşturma ve raporlama aşamalarını kapsayan denetim sürecine ilişkin hususların mevzuat kapsamında belirgin olması gerekmektedir.

Bu çalışma ile yapılan mevzuat taraması neticesinde, denetim usullerine, 5070 sayılı Elektronik İmza Kanunu, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelik kapsamında genel olarak yer verildiği, ancak düzenleme noktasında bazı eksikliklerin olduğu veya bazı hususların geliştirilmesi gerektiği tespit edilmiştir.

Örneğin; 5070 sayılı Elektronik İmza Kanunu ve Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik kapsamında; planlama, inceleme, önaraştırma, soruşturma ve raporlama aşamalarını kapsayan denetim sürecine ilişkin hususlarda herhangi bir düzenleme bulunmamaktadır. Ayrıca, Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelik ile hüküm altına alınmış olan ön araştırma ve soruşturma aşamalarına ilişkin düzenlemelerin geliştirilmesi gerektiği düşünülmektedir.

Aşağıda maddeler halinde belirtilen hususlara ilişkin düzenlemelerin, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelik çerçevesinde veya TK'nın tüm denetim yetkileri için uygulanabilir denetim süreçlerinin belirlendiği, denetime ilişkin hükümleri tek çatı altında toplayan genel denetim mevzuatı kapsamında yapılması gerektiği değerlendirilmektedir.

Dördüncü bölümde denetim usullerine ilişkin uygulanması gereken süreçler açıklanmıştır. Söz konusu açıklamalar çerçevesinde, mevcut mevzuatta düzenlenmeyen veya geliştirilmesi gerektiği tespit edilen hususlara aşağıda değinilecektir:

o Denetimin etkinliği ilkesinin denetim çalışmalarına birçok yansımaları bulunmaktadır. Zira denetimin etkinliğini etkileyen birçok faktör bulunmaktadır. Örneğin, denetim görevlisinin, denetim sürecinde sorumluluklarını doğru bir şekilde yerine getirilebilmesi için gerekli teknik bilgiye, eğitime ve mesleki yeterliliğe sahip olması, denetimin istenen etkinlikte olabilmesini ve denetim sonunda tam ve doğru bir görüş bildirilebilmesini teminen, denetim görevlisi tarafından yapılan işin her seviyede gözden geçirilmesi, konuyla ilgili tecrübesi ve bilgisi bulunan kişi veya kuruluşlardan görüş alınması, denetime çıkmadan evvel daha önceki denetim raporlarının dikkate alınması ve daha önceki önerilerin yerine getirilip getirilmediğinin kontrol edilmesi gibi hususlar denetimin etkinliğini etkileyen başlıca faktörler arasında yer almaktadır. Bu itibarla, denetimin etkinliği ilkesinin denetim ilkeleri kapsamı altında düzenlenmesinin faydalı olacağı mütalaa edilmektedir.

o Denetim çalışmalarının verimli bir şekilde yürütülmesi noktasında, denetim hazırlık çalışmalarının yapılması büyük önem taşımaktadır. Bununla bağlantılı olarak; çalışmaların ekip halinde yapılması halinde, ekibe dahil denetim görevlilerinden ilgili Daire Başkanlığının personeli arasından unvan olarak en yüksek olan kişinin, aynı unvanda birden fazla kişi olması halinde ise bu unvanda hizmet yılı en fazla olan denetim görevlisinin ekip başkanı olarak belirlenmesi, elektronik imza

mevzuatının taranması, geçmişte hazırlanmış denetim raporlarının incelenmesi, bu raporlarda belirtilen hususların yerine getirilip getirilmediğinin kontrol edilmesi ve ESHS'nin kurumsal yapısı hakkında bilgi toplanması denetim hazırlık çalışmaları kapsamında yapılması gereken işlerdir. Bu çerçevede, denetim hazırlık çalışmalarına ilişkin hususların mevzuat kapsamında düzenlenmesi gerekmektedir.

o İnceleme aşaması, ESHS'nin denetime tabi faaliyetlerinin ilgili mevzuata uygun olup olmadığını tespit etmek üzere dosya üzerinde ve/veya yerinde yapılan işlemleri kapsamakta ve denetim sürecinin en önemli adımını teşkil etmektedir. Bu aşama, denetim yöntemlerinin uygulanarak, güvenilir sonuçlar çıkarmaya elverişli, uygun ve yeterli miktarda denetim delillerinin toplandığı bir aşamadır. Denetim raporunda yer alacak tespitlerin dayanak noktası olması, diğer bir deyişle, denetim çalışmalarının temelini teşkil etmesi yönüyle büyük önem taşıyan inceleme aşamasının mevzuat çerçevesinde düzenlenmesi gerekmektedir.

o Ön araştırma, denetlenen taraf hakkında soruşturma açılmasına gerek olup olmadığının tespiti için öngörülen bir ara süreçtir. Ön araştırma aşaması Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelik kapsamında düzenlenmiş olup, ön araştırma yapılmasına Kurulun karar verebileceği ve ön araştırma yapılmasına karar verdiği takdirde Kurulun, Kurum çalışanlarından bir ya da birkaçını görevlendireceği hüküm altına alınmıştır. Ancak, Kurul tarafından, ön araştırma yapmak üzere, ilgili Daire Başkanlığının görevlendirilmesi ve ilgili Daire Başkanlığı tarafından yapılacak görevlendirme ile "denetim görevlisi" vasfını kazanan personel tarafından hazırlanacak ön araştırma raporunun Kurula sunulması suretiyle ön araştırma aşamasının düzenlenmesinin, denetim çalışmalarının en kısa sürede bitirilmesi ve denetim çalışmalarının verimli bir şekilde yürütülmesi bakımından daha uygun olacağı değerlendirilmektedir.

o Soruşturma, yapılan incelemeler neticesinde denetlenen tarafla ilgili tespit edilen hususların daha ayrıntılı şekilde tahkik edildiği bir aşamadır. Soruşturma aşaması Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Usul ve Esasları Hakkında Yönetmelik kapsamında düzenlenmiş olup, Kurulun, soruşturma yapmak üzere Kurum Başkan Yardımcısı veya Daire Başkanlarından birinin başkanlığında

Kurum personelinden oluşan bir heyeti görevlendireceği hüküm altına alınmıştır. Ancak, Kurul tarafından, soruşturma yapmak üzere, ilgili Daire Başkanlığının görevlendirilmesi, ilgili Daire Başkanlığı tarafından yapılacak görevlendirme ile "denetim görevlisi" vasfını kazanan personel tarafından soruşturma raporunun hazırlanması, soruşturma raporu ve ESHS'nin yazılı savunmasından oluşan soruşturma dosyasının denetim görevlisi tarafından ivedilikle değerlendirilmesi, söz konusu değerlendirme sonucunda, ESHS hakkında idari yaptırım ve tedbirlerin uygulanmasına ilişkin denetim görevlisi kanaatinin soruşturma raporuna derc edilmesi, ilgili Daire Başkanlığı amiri tarafından soruşturma raporunun Kurula sunulması ve Kurul tarafından idari yaptırım ve tedbirlerin uygulanmasına veya uygulanmamasına karar verilmesi suretiyle soruşturma aşamasının düzenlenmesinin daha uygun olacağı değerlendirilmektedir.

- **Periyodik Denetimlerin Uygulanması**

Yönetmeliğin 22 nci maddesinde *"ESHS'nin denetimi Kurum tarafından gerek görülmesi halinde ve iki (2) yılda en az bir defa re'sen yapılır."* hükmü yer almaktadır.

Elektronik imza mevzuatına ilişkin düzenlemelerin yürürlüğe girmesiyle, elektronik imza konusunda düzenleyici kurum olan TK'ya düşen en önemli görev; ESHS'lerin, bu düzenlemelere uygun faaliyette bulunup bulunmadıklarını periyodik olarak denetlemektir. Zira tüketici haklarının korunması, ESHS'ler arasında sürdürülebilir rekabetin sağlanması ve sertifika pazarının gelişimi yönünde tedbirler alınması için etkin bir denetim mekanizmasının oluşturulması büyük önem taşımaktadır. Bu nedenle, TK'nın denetim fonksiyonunun en iyi şekilde işlemesi ayrı bir önem kazanmaktadır. TK tarafından denetim işlevinin etkin bir şekilde yerine getirilmesi ve bu durumun ESHS'ler tarafından hissedilmesi, ESHS'lerin elektronik imza mevzuatı hükümlerine dikkatli bir şekilde riayet etmeleri sonucunu doğuracaktır.

Bu itibarla, denetimin etkinliği ve verimliliği açısından, elektronik imza mevzuatına uygun olarak, ESHS'lerin yılda bir defa periyodik olarak denetlenmesinin yerinde olacağı değerlendirilmektedir.

KAYNAKLAR

[1] Sarıkaya, K.S., 2005, Elektronik İmza Güvenliği ve Güvenlik Standartları Çerçevesinde Düzenleyici Yaklaşımlar, Telekomünikasyon Kurumu Uzmanlık Tezi, Ankara

[2] Sağıroğlu-Alkan, 2005, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara

[3] E-Dönüşümün Anahtarı, http://www.e-imza.gen.tr, 07.09.2006

[4] Electronic Signatures in Global and National Commerce Act, http://www.ftc.gov/os/2001/06/esignreport.pdf, 07.09.2006

[5] Tulloch M., 2003, Microsoft Encyclopedia of Security, Microsoft Press

[6] TÜBİTAK UEKAE, 2004, Açık Anahtar Altyapısı ve Elektronik İmza Uygulamaları Eğitim Kitapçığı

[7] E-Tuğra, http://www.e-tugra.com, 08.09.2006

[8] Telekomünikasyon Kurumu, http://www.tk.gov.tr/Tuketici/Sorulanlar/Sorulanlar.htm, 08.09.2006

[9] Rüssmann, H., 2002, İnternette Hukuki İşlemler: Hukuki Geçerliliği ve İspat Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir

[10] Centre for Applied Cryptographic Research (CACR) at the University of Waterloo,http://www.cacr.math.uwaterloo.ca/hac/about/chap1.pdf,11.09.2006

[11] Özgül, E. M., İnternette hukuki güvenlik ve dijital imza, http://inet-tr.org.tr/inetconf8/bildiri/141.doc, 12.09.2006

[12] Sözer, B., 2002, Elektronik Sözleşmeler, Beta Yayınları, İstanbul

[13] Şenocak, Z., 2001, Dijital imza ve dijital imzanın Borçlar Kanunu hükümleri açısından ele alınması, AÜHFD, Ankara

[14] RSA Security, http://www.rsasecurity.com, 13.09.2006

[15] Gradkell Systems, http://www.gradkell.com/PKI/sld003.htm, 15.09.2006

[16] Berber Keser L., 2001, Şekil ve dijital imza, Ankara

[17] The Keys of Cryptography, http://www.ati.es/novatica/UPGRADE/issues/2004/6/upgrade-vol-V–6.pdf, 14.09.2006

[18] E-Güven Nitelikli Elektronik Sertifika Uygulama Esasları Sürüm 1.1 Yürürlük Tarihi: Kasım, 2005 OID: 2.16.792.3.0.1.1.2.1

[19] Açık Anahtar Altyapısı Eğitim Kitabı, https://www.kamusm.gov.tr/net/bilgiler/teknik/aaa/index.html?kisaltmalarvetanimlar.html, 18.12.2006

[20] Açık Anahtar Altyapısı, http://www.e-guven.com, 07.09.2006

[21] WEBOPEDIA, http://www.webopedia.com/TERM/P/PKI.html, 14.09.2006

[22] Virginia Tech Certification Authority, http://www.pki.vt.edu/help/faq/general_faq.htm, 14.09.2006

[23] Bakırcı, Y., Elektronik İmza Kanunu çerçevesinde yetki ve bildirim, http://www.eimza.gen.tr/templates/resimler/File/makaleler/Elektronik_imza_kanununda_Yetki_Yasin_BAKIRCI.doc, 14.09.2006

[24] ABA, American Bar Association, http://www.abanet.org/scitech/ec/isc/dsgfree.html, 14.09.2006

[25] Rivest, R L., http://theory.lcs.mit.edu/ rivest, 14.09.2006

[26] Adams, C., Lloyd, S., 2002, Understanding PKI Concepts, Standards and Deployment Considerations, Addison Wesley Professional

[27] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, http://ftp.rfc-editor.org/in-notes/rfc2527.txt, 18.09.2006

[28] Lannerstrom, S., 2000, Basic Elements of a PKI, Sonera SmartTrust Ltd.

[29] Bakırcı, Y., 2005, Uyumlu Çalışabilirlik Modelleri ve Türkiye İçin Durum Değerlendirmesi, Yayınlanmamış Çalışma

[30] Kenger, E., 2001, Yüksek Denetleme Kurulu Denetçi Yardımcıları Eğitim Notu, http://www.ydk.gov.tr/egitim_notlari/denetim.htm, 23.08.2006

[31] Aykın, H., Denetim, denetim standartları ve denetim süreci, Ankara

[32] Türk Dil Kurumu, http://www.tdk.org.tr, 23.08.2006

[33] Aksoy, T., 2006, Tüm Yönleriyle Denetim, Yetkin Yayınları, Ankara

[34] Türker M., Pekdemir R., Uluslararası denetim standartları, Türkiye uygulaması ve beklentiler, http://www.semor.com.tr/misc/muhasebe/turker-pekdemir_bildiri.html, 29.01.2007

[35] NAFE, http://nafe.net/LER/l1_2_5.pdf, 24.08.2006

[36] Güredin, E., 2000, Denetim, Beta Yayınları 10.Baskı, İstanbul

[37] 26.12.1992 tarihli ve 21447 sayılı Resmi Gazete'de yayımlanan Muhasebe Sistemi Uygulama Genel Tebliği sıra no:1

[38] Kepekçi, C., Şubat 2000, Bağımsız Denetim, Siyasal Kitabevi, 4. Baskı, Ankara

[39] Gürbüz H., 1990, Muhasebe Denetimi, İstanbul

[40] Enerji Piyasasında Faaliyet Gösteren Gerçek ve Tüzel Kişilerin Bağımsız Denetim Kuruluşlarınca Denetlenmesi Hakkında Yönetmelik, http://www.mevzuat.adalet.gov.tr/html/21611.html, 20.09.2006

[41] Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ, http://rega.basbakanlik.gov.tr/index.aspx#, 22.09.2006

[42] 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, http://www.bumko.gov.tr/mevzuat/Kanunlar/5018.htm, 20.09.2006

[43] Stetler, H F., 1982, Auditing Principles, A System Based Approach, Prentice-Hall Inc., New Jersey

[44] Cook John W., Gary, M., 1980, Auditing, Philosophy and Technique, Hougton Mifflin Company, Boston

[45] AICPA, American Institute of Certified Public Accountants, Code of Professional Ethics

[46] Official Journal of the European Communities, 2000, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[47] Türkoğlu, Y., Bilgi çağında elektronik ticaretin dış ticarete etkileri, http://www.igeme.org.tr/, 05.10.2006

[48] Alkan, M., Özenç K., E-ticaretten m-ticarete doğru süreçteki yeni yansımalar

[49] FESA, Forum of European Supervisory Authorities for Electronic Signatures, www.fesa.art.at, 02.01.2007

[50] Sevim, T., Elektronik imzanın hukuksal boyutları mevcut durum, eksiklikler ve çözüm önerileri

[51] LEUVEN Katholieke Universiteit, The Legal and Market Aspects of Electronic Signatures

[52] IDABC, e-government in Germany, http://ec.europa.eu/idabc/servlets/Doc?id=21010, 23.11.2006

[53] Information Society Germany 2006, http://www.bmbf.de/pub/aktionsprogramm_2006_gb.pdf, 23.11.2006

[54] Act on Digital Signature (Gesetz zur digitalen Signatur), http://www.iuscomp.org/gla/statutes/SiG.htm#ToC13, 19.10.2006

[55] Digital Signature Ordinance (Signaturverordnung - SigV) http://www.datenschutz-berlin.de/recht/de/rv/tk_med/sigve.htm, 19.10.2006

[56] RegTP's Tasks, 2005, Almanya Eğitim Çalışmaları Powerpoint Presentation

[57] TÜV Informationstechnic GmbH, Examination and Attestation of CPSs According to the German Digital Signature Act

[58] Electronic Signatures Implementation, 2005, Almanya Eğitim Çalışmaları Powerpoint Presentation

[59] Center of Administrative Innovation in the Euro-Mediterranian Region, Best Practices in the European Countries: The Netherlands

[60] European Commission e-Government Unit, Top of The Web Survey on quality and Usage of Public e-services

[61] The Digital Economy 2005, http://www.cbs.nl/nr/rdonlyres/cb06d0dc890548e4b1d9a54f790ab215/0/2006p38pub.pdf, 17.10.2006

[62] Electronic Signature Act, http://www.elo.nl/elo/Images/wet_elekhandtek_stb_tcm70-56809.pdf, 17.10.2006

[63] CHRONOPAY, http://www.chronopay.com/en/legal_psp, 12.10.2006

[64] WEBTRUST, http://www.webtrust.org/abtseals.htm, 12.10.2006

[65] OPTA, 2006, Electronic Signatures General Information

[66] OPTA, 2004, Vision of the Market Annual Report

[67] Raad Voor Accreditatie, http://www.rva.nl/,12.10.2006

[68] ECP. NL, 2002, Scheme for Certification of Certification Authorities against ETSI TS 101 456

[69] Europe's Information Society, http://europa.eu.int/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm, 04.12.2006

[70] KPMG, http://www.kpmg.nl/site.asp?id=34757, 16.10.2006

[71] Sauer, J., 29 May-1 June 2006, Training Telecommunications Authority

[72] PINKROCCADE, http://www.pki.pinkroccade.com, 13.10.2006

[73] DIGINOTAR, http://www.diginotar.nl/, 13.10.2006

[74] Canbay, C., 29 Mayıs-1 Haziran 2006, Hollanda Eğitim Notları

[75] UZIREGISTER, http://www.uziregister.nl/, 13.10.2006

[76] RIDE, A Roadmap for Interoperability of eHealth Systems in Support of COM 356 with Special Emphasis on Semantic Interoperability, http://www.srdc.metu.edu.tr/webpage/projects/ride/deliverables/RIDED.2.1.1%20CurrentPracticesDutch.doc, 13.10.2006

[77] KADO, http://www.koil.or.kr/mypage/, 09.08.2006

[78] Republic of Korea e-Commerce, http://www.ecommerce.or.kraboutec_issue4.asp, 24.11.2006

[79] Kyubeom, C., LL.D., Electronic Signature Act and PKI Status in Korea

[80] JETRO, http://www.jetro.go.jp/en/stats/survey/surveys/b2c/korea.pdf, 08.08.2006

[81] KISA, http://www.kisa.or.kr/kisae/kcac/jsp/kcac_20_10.jsp, 08.08.2006

[82] KICA, http://www.signgate.com/eng/e_support/e_sup03.htm, 08.08.2006

[83] YUN, 2002, Jae Suk, PKI Scheme in Korea, Korea PKI Forum

[84] NIASIGN, http://sign.nia.or.kr/, 24.11.2006

[85] YESSIGN, http://www.yessign.or.kr/, 09.08.2006

[86] SIGNKOREA, http://www.signkorea.com/eng/index.php, 23.11.2006

[87] CROSSCERT, http://www.crosscert.com/service_gcca/Main.jsp, 24.11.2006

[88] TRADESIGN, http://www.tradesign.net/, 24.11.2006

[89] Eken, C., 2002, Ulusal Telekomünikasyon Düzenleme Kurumları: Kurumsal Yapı ve Sorumlulukları ile Denetleme ve Yaptırım Uygulama Fonksiyonları, Telekomünikasyon Kurumu Uzmanlık Tezi, Ankara

[90] Gözübüyük, A. Ş., Tan, T., 2001, İdare Hukuku, Genel Esaslar, Turhan Kitabevi, Cilt 1, Güncelleştirilmiş 2. Bası, Ankara.

[91] Akbıyık, S., 2005, Vergi Uygulamaları Yönüyle Denetim ve Raporlama, Ekin Kitabevi

[92] 12.08.2001 tarihli ve 24491 sayılı Resmi Gazete'de yayımlanan Sermaye Piyasası Mevzuatı Çerçevesinde Değerleme Hizmeti Verecek Şirketlere ve Bu Şirketlerin Kurulca Listeye Alınmalarına İlişkin Esaslar Hakkında Tebliğ

[93] Erdoğan M., Şubat 2005, Denetim, Maliye ve Hukuk Yayınları

[94] Bağımsız Denetim İlkelerine İlişkin Yönetmelik, http://www.bddk.org.tr/turkce/mevzuat/603Bagimsiz_denetim_ilkeleri_hk_yonetmelik.doc, 29.01.2007

[95] British Columbia Genel Denetçilik Kurumu, Performans Denetimi Kılavuzu,http://www.ydk.gov.tr/performans_denetim/denetimlerin_planlanmasi.htm, 06.09.2006

[96] http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=53, 23.08.2006

[97] BSI, 2005, Information Security Management System Auditor Course Student Manual

[98] Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik, http://www.sigortacilik.gov.tr/02YD/21TSM/21.03Yonetmelik/SBD_ilkelerine_iliskinY.pdf, 06.09.2006

[99] Tarlan, S., Gül, Ş., Tosun, E., 7.2.2003 tarihli ve 1,4,19 sayılı Basit Rapor

[100] Yazıcı, K., Sümer, N., İlter, K., Arslan, S., Ulaşanoğlu, E., Temmuz 2005, Telekomünikasyon Sektöründe Denetim, Karşılaşılan Zorluklar ve Çözüm Önerileri, Telekomünikasyon Kurumu, Ankara

[101] ETSI TS 101 456 V1.4.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[102] KOBİ, www.kobitek.com, 20.09.2006

[103] BS ISO/IEC 27001:2005 Information technology - Security techniques-Information security management systems-Requirements

[104] SAFENET, The Foundation of Information Security, http://www.safenetinc.com/solutions/ent/pki/keyMgt.asp, 21.09.2006

[105] Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu Raporu 2004, İstanbul

[106] CWA 14167–1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

[107] Beydoğan, A., 2005, Elektronik Sertifika Pazarı ve Rekabet, Telekomünikasyon Kurumu, Ankara

[108] Günday M., 2002, İdare Hukuku, 6. Aynı Bası, Ankara

[109] IPA, 2005, Electronic Signature Laws, PKI Projects and Time Stamping Technology in the European Union and Germany

ÖZGEÇMİŞ

1976 yılında İstanbul'da doğdu. İlk, orta ve lise öğrenimini İstanbul'da tamamladı. 2000 yılında İstanbul Üniversitesi Hukuk Fakültesinden mezun oldu. 4 Ağustos 2001 tarihinden 4 Aralık 2003 tarihine kadar Turizm Bakanlığı'nda Müfettiş Yardımcısı olarak görev yaptı. 4 Aralık 2003 tarihinde Telekomünikasyon Uzman Yardımcısı olarak girdiği Telekomünikasyon Kurumu'nda Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığında çalışmaktadır. Evli olup, iyi derecede İngilizce bilmektedir.