ELEKTRONİK İMZA UYGULAMASINDA KULLANILAN ZORUNLU VE İHTİYARİ DOKÜMANLAR

TUĞRUL SEVİM
103615073

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
EKONOMİ HUKUKU YÜKSEK LİSANS PROGRAMI

TEZ DANIŞMANI: YRD. DOÇ. DR. LEYLA KESER BERBER
2006

İÇİNDEKİLER

Sayfa No

KISALTMALAR

AAA	Açık Anahtar Altyapısı
AICPA/CICA	American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants.
BK	Borçlar Kanunu
Bkz.	Bakınız
CA	Certification Authority (Sertifika Otoritesi)
CEN	European Committee for Standardisation
COBIT	Control Objectives for Information and Related Technologies
EC	European Commission
ETSI	European Telecommunications Standards Institute
f.	Fıkra
FIPS	Federal Information Processing Standards
HUMK	Hukuk Usulü Muhakemeleri Kanunu
ISACA	Infornation Systems Audit and Control Association
İİK	İcra İflas Kanunu
ITSEC	Information Technology Security Evaluation Criteria
md.	Madde
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFC	Request For Comments
RSA	Rivest, Shalmir, Adleman
SigG	Signaturgesetz (İmza Kanunu)

GİRİŞ

5070 sayılı Elektronik İmza Kanunu'nun yürürlüğe girmesinden sonra, elektronik imza uygulamasının başlayabilmesi için gerekli ikincil mevzuatın tamamlanması bekleniyordu. Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, çeşitli Yönetmelik değişiklikleri ve en son konuyla ilgili Kurul Kararı'nın çıkmasına rağmen ülkemizde hala gerektiğince elektronik imza uygulaması geliştirilememiş bulunmaktadır. Kamuda sadece bir elektronik imza uygulaması geliştirilmiş, özel sektörde ise birkaç firma elektronik imza uygulaması için gerekli alt yapı yatırımlarını tamamlamışlardır. Bu tablo elektronik imza uygulaması için umut kırıcı olmakla beraber, hali hazırda planlaması ve teknik çalışmaları sürdürülen çok büyük boyutlarda elektronik imza projeleri de bulunmaktadır. Bu projelerin hayata geçirilmesi ile birlikte elektronik imza hem ticari hayatta hem kamu-vatandaş ilişkisinde her gün kullanılır hale gelecek bir teknoloji halini alacaktır. Bu çalışma ile şimdiye kadar elektronik imzanın hukuki boyutu ve delil değeri üzerine yapılan çalışmalardan farklı olarak, elektronik imzanın teknik özellikleri doğrultusunda hukuki altyapısı ortaya konulacaktır.

Elektronik imza uygulamasının hukuki altyapısının ortaya konulmasında elde bulunan en önemli argümanlar elektronik imza uygulamasında kullanılan ihtiyari ve zorunlu dokümanlardır. Niteliklerine göre teknik yapısı değişen elektronik imza uygulamasında, bu nitelikler kendilerini ortaya konulan dokümanlar ile göstermektedirler. Bu çalışmada öncelikle basit bir şekilde elektronik imzanın ve bileşenlerinin teknik açıklamaları yapıldıktan sonra elektronik imza uygulaması katılımcıları ve ilgili sorumluluk yapısı incelenecek ve söz konusu dokümanların içerik çerçeveleri ve hukuki statüleri tartışılarak uygulamada çıkan ve çıkması muhtemel olan sorunlara çözüm önerileri getirilecektir.

BİRİNCİ BÖLÜM

ELEKTRONİK İMZA UYGULAMASININ TEMEL ÖZELLİKLERİ

A. ELEKTRONİK İMZANIN TEKNİK ÖZELLİKLERİ

Elektronik imza terimi, genellikle, elektronik ortamdaki irade beyanlarının tümü için kullanılan bir tanımdır. Geniş bir tanım yapmak gerekirse, elektronik imza, bir belgeyi imzalama niyetinde olan bir kişi tarafından sahiplenilmiş ya da icra edilmiş bir belgeyle/kayıtla mantıksal bir şekilde ilişkilendirilmiş veya eklenmiş bir süreç, elektronik bir ses, veya sembol anlamına gelir[1].

Bu tanımla,

- PIN veya Parola
- Biometrik Veri
- Yazılımın metin kutusunu işaretleme/tıklama
- İsim Yazma
- Dijital ortama geçirilmiş elle atılmış imza
- Dijital İmza veya diğer şifreleme bazlı tanımlama sistemleri
- Bilgi/kişisel veri bazlı tanımlama

elektronik imza olarak kabul edilebilecektir.

Dünyada elektronik imza ile ilgili hukuki düzenlemelerde de, yukarıdaki tanım geniş olarak alınmakta veya sınırlı bir şekilde yorumlanmaktadır. Yorumun sınırlı veya

[1] UETA, Uniform Electronic Transactions Act (1999)

geniş yapılmasına göre düzenleme kapsamındaki elektronik imzaların hukuki statüleri değişmektedir. Bu düzenleme yaklaşımları üç şekilde sınıflandırılabilir[2];

- Minimalist Yaklaşım

Herhangi bir teknolojiyi tanımlamadan kanunda belirtilen belli şartları yerine getiren her türlü elektronik imza çeşidi ıslak imza ile aynı hukuki statüde sayılır. (UETA; E-Sign)

- Emredici Yaklaşım

Düzenlemeler Açık Anahtarlı Alt Yapı (AAA, PKI) üzerine kurulur; Sertifika Hizmet Sağlayıcıları üzerine ağır mali ve hukuksal yükümlülükler yüklenir; elektronik imzanın hukuksal geçerliliği ancak belli koşullar altında tanınır (Kara Avrupası Hukuk Sistemine sahip olan ülkeler -İtalya, Almanya, Arjantin-, Utah Eyaleti Dijital İmza Kanunu, 5070 Sayılı Elektronik İmza Kanunu)

- Karma Yaklaşım

En fazla kullanılan kimlik kanıtlama teknolojileri minimum düzeyde kabul görürken bunun yanında dijital imzalarla ilgili hükümler düzenlemeler içersine yerleştirilir. (Avrupa Birliği, UNCITRAL Model Law on Electronic Signatures, U.S. State of Illinois)

5070 sayılı Elektronik İmza Kanunu da emredici yaklaşımı benimseyen düzenlemelerdendir. Buna göre sadece AAA sistemini ile oluşturulmuş ve yetkili ESHS tarafından yayınlanan elektronik sertifikalar ile en az EAL4 güvenlik seviyesindeki kripto cihazları ile oluşturulmuş imzalar hukuken elle atılmış imza ile aynı sonucu doğurmaktadır; ve bu elektronik imza, güvenli elektronik imza olarak adlandırılmıştır.

[2] Mason, S. Electronic Signatures in the EU and world e-commerce: technical and legal ramifications, 1999, http://www.itsecurity.com/archive/papers/digsig.htm

Kanunda diğer yollarla yaratılan elektronik imzalar için bir hukuki değer belirlenmemiştir.

5070 sayılı Elektronik İmza Kanunu'nun sadece AAA destekli elektronik imzaları tanıması sebebiyle, bu çalışmada sadece AAA sisteminin temel teknik özellikleri incelenecektir.

I. Açık Anahtarlı Alt Yapı – AAA (Public Key Infrastructure–PKI) Sistemi

AAA Sistemi matematiksel olarak birbirleriyle eşsiz uyum gösteren bir çift sayısal anahtarın simetrik olarak şifreleme fonksiyonu yerine getirmek amacıyla kurgulanması mantığına dayanır. AAA sisteminin bir örnekle fonksiyonel bir tanımını yapmak gerekirse;

" ... AAA, elektronik ticaret işlemlerinde tarafların, dijital sertifikalar yardımıyla kimlik kanıtlamayı sağlayacak şekilde birbirlerini tanımlayabilmelerini, kriptoloji, kimlik kanıtlama ve bütünlük kullanılarak ticari iletişimin gizliliğinin ve uygun bir tabanda dijital imza yardımıyla da iletişimin inkar edilemezliğinin sağlandığı platformdur."[3]

AAA, bütünlük, kimlik kanıtlama, inkar edilemezlik gibi nitelikleri sebebiyle elle atılmış imzanın özelliklerini en fazla karşılayan teknolojidir. AAA, sisteme girme, şifreleme ve dijital imzalama gibi çeşitli fonksiyonlara sahiptir[4].

[3] AICPA/CICA, WebTrust Program for Certification Authorities, Vs. 1.0, 25 August 2000, s, 10-11
[4] Kiran S., Lareau P., Lloyd S., PKI Basics - A Technical Perspective, PKI Forum, November 2002

II. AAA Sisteminin Fonksiyonları

1. Kimlik Kanıtlama (Authentication)

Bir sitemle iletişim kuran veya işlem yapan kimsenin doğrulanmasının sağlanması yeteneğine kimlik kanıtlama denir[5]. Mesaj kimden geldi veya gelen mesaj hakiki bir mesaj mı yoksa sahte bir mesaj mı sorularına cevap alınmasını sağlayan AAA sisteminin bu fonksiyonu, dijital sertifika ile birlikte sağlanmaktadır. Dijital sertifika, günlük hayatta kullanılan kimlik kartlarının elektronik ortamdaki karşılığıdır. Dijital sertifika kişinin kimliğini ve söz konusu bilgiye veya online hizmete ulaşım hakkını kanıtlamak için elektronik olarak ibraz edilmek üzere geliştirilmiştir. Dijital sertifikalar dijital bilgileri şifrelemek ve şifrelenen bilgileri çözmek için kullanılan bir çift elektronik anahtar ile kimlik bilgisini bağlar. Dijital sertifika kullanıcıların ve kuruluşların bilgilerinin iletişim ağlarında güvenli bir şekilde iletilmesini sağlar. Dijital sertifikada kullanıcıya ait açık anahtar, kullanıcının adı, son kullanma tarihi sertifikanın alındığı kurumun adı ve seri numarası bulunur.

2. Bütünlük (Integrity)

Bütünlük fonksiyonu iletişimin hatalı veya kasıtlı olarak değiştirilmesini engeller[6]. Alıcının aldığı doküman, göndericinin gönderdiği dokümanla aynı mı, gönderim işlemi tamamlandı mı ve doküman depolanma veya gönderilme sırasında

[5] Stapleton J., Biometrics, PKI Forum, May 2001, s.1

[6] Hindelang S., No Remedy for Disappointed Trust – The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared, Journal of Information, Law and Technology, March 2002

değişime uğradı mı gibi sorular bu başlık altında yanıt bulmaktadır. İnternet gibi açık ağ sistemlerinde gönderilen mesajın iletim kanalları içersinde başkaları tarafından görüntülenmesi, değiştirilmesi veya iletiminin engellenmesi mümkündür. Mesajın bütünlüğü özellikle açık ağ yapıları içersinde yapılan iletişime olan tarafların güvenini sağlaması açsından önemli bir fonksiyonu yerine getirmektedir.

3. İnkar Edilemezlik (Nonrepudiation)

İnkar edilemezlik iletilen mesajın göndericisi tarafından iletildiğinin kanıtlanmasına yarar. Mesajı gönderen yukarıdaki özellikleri taşıyan mesajı göndermediğini ve bu mesajın kendisinden sadır olmadığını bu fonksiyon sayesinde iddia edemez[7]. Bu durum ayrıca elektronik ticaret açısından da büyük bir önem taşımaktadır. Zira gönderilen mesajın inkar edilemezlik özelliğine sahip olması elektronik ortamda sözleşmenin kurulması ve niyet mektuplarının muhatabı tarafından dikkate alınması hususlarında da taraflara yeterli güveni verebilecektir.

III. AAA Sisteminin İşleyişi

AAA sisteminin fonksiyonlarını açıkladıktan sonra bu sistemin işleyişi hakkında bilgi verebiliriz. AAA sistemi matematiksel anlamda birbirleriyle eşsiz bir uyum içersinde olan iki adet anahtardan oluşmaktadır. Bu anahtar çiftinden (key pair) açık olan kamu tarafından erişilebilir iken kapalı olan yalnızca anahtar çifti sahibi tarafından bilinmektedir. Açık anahtar kriptolojisi, basit olarak mesajın bu anahtar çiftlerinden biri ile şifrelenip diğeri ile deşifre edilmesi mantığına dayanmaktadır[8]. Örnek vermek gerekirse bilgisayarınızda yarattığınız elektronik bir

[7] Performance Engineering Corporation, Public Key Infrastructure Analysis, PEC Solutions, Inc.Virginia, March 2000

[8] Ribagorda-GarnachoA.,Electronic Signature at the Heart of Information Security Developpement: An Overview", UPGRADE Vol. V, No. 3, June 2004 s. 8

dosyayı kamuya açık olan herkesçe öğrenilebilen alıcının kapalı anahtarı ile şifrelerseniz mesajı yalnızca alıcı açabilecektir. Zira bu açık anahtarla şifrelenmiş olan dosyayı deşifre etmek sadece alıcının kapalı anahtarıyla mümkün olacaktır[9].

Bu durumda alıcı yukarıda sayılan AAA sisteminin bütünlük fonksiyonunu yerine getirmiş olacaktır. Ancak bu durumda AAA sisteminin inkar edilemezlik ve kimlik kanıtlama fonksiyonlarının da gerçekleştirildiğinden bahsedilemez. Zira alıcının açık anahtarıyla şifrelenmiş olan mesajı herkes yaratabilir ve bu mesaj gönderenin kimliği ve mesajın gerçekten alıcıya ulaşan şekilde gönderici tarafından gönderildiği de iddia edilememektedir. Oysa mesaj göndericinin kapalı anahtarıyla şifrelenmiş olsaydı, alıcı kamuya açık olan göndericinin açık anahtarıyla bu mesajı deşifre edebilecek mesajın kapalı anahtarın sahibi olarak bilinen kişi tarafından gönderildiği kanıtlanmış olacaktır.

IV. Dijital İmza

Dijital imza yukarıda açıklamaya çalıştığımız AAA Sisteminin bütün fonksiyonlarını gerçekleştiren ve asimetrik tarzda çalışan bir şifreleme tekniğidir. Dijital imza asimetrik işleyiş yapısıyla yani göndericinin kapalı anahtarı ile alıcının açık anahtarın aynı şifreleme işleminde eşzamanlı olarak kullanıldığı, bunun yanında mesajın şifrelenmesi sırasında parçalanması ve deşifre edilme aşamasında tekrar birleştirilmesi (hashing) uygulamasının da dahil olduğu bir platformu ifade etmektedir[10].

---

[9] Yıldız E., A Propsal For Turkish Government Public Key Infrastructure Trust Model, December 2001, s. 8

[10] Yıldız E., A Propsal For Turkish Government Public Key Infrastructure Trust Model, December 2001, s. 10

Hashing (sıkıştırma) işlemi öyle bir işlemdir ki, bununla sıkıştırdığınız veriler (hash value), yani evraka yazdıklarınız, adeta bir sürü yerinden yırtılıp bir küçük boyuta (message digest, mesaj özeti) indirilmekte bir tür yığın teşkil etmektedir.

Hashing sonucu elde edilen matematik algoritmik değere; hash value adı verilir. Hash value en büyük özelliği sözkonusu döküman ile sıkı sıkıya bağlı oluşudur. Şöyle ki, o doküman yanlız bir tek tip hash value sonucunu mümkün kılabilir ve ve bir hash value sadece bir tek dokümana uygulanabilir. Böylece bir kere digital olarak imzalanmakla, dokümanı üzerinde değişiklik yapılması imkansız olmaktadır. Diğer bir deyişle bir dokümanı tamamlayıp imzaladığınızda oluşan hash değeri, mesaj özeti, onu üreten - ve sayısal imzanızı içeren-bilgisayara özel olarak, geri dönüşsüz ve eşsiz (unique) olarak oluşmaktadır.

B. ELEKTRONİK İMZA UYGULAMASINDA İLGİLİ TARAFLAR

Elektronik imza uygulamasında farklı işlevlere ve farklı hak ve yükümlülüklere sahip taraflar bulunmaktadır. Elektronik imza uygulamasının özelliklerine göre katılan taraflar değişebilecek olmasına rağmen her uygulamada en azından, elektronik sertifika hizmet sağlayıcı (kayıt makamı ile birlikte), imzalayan ve doğrulayan bulunmaktadır. Elektronik imza uygulamasının bir topluluk uygulaması olması veya üçüncü bir taraf tarafından sağlanıyor olması halinde, uygulama sağlayıcı ve/veya ilke/politika belirleyici de taraflar arasında sayılabilecektir. Ayrıca uygulamada dinamik bir etkileri olmamasına rağmen elektronik imza ürün sağlayıcıları (güvenli elektronik imza oluşturma aracı, güvenli elektronik imza doğrulama aracı, güvenli elektronik imza oluşturma uygulamalarında kullanılan yazılımlar) da çeşitli yükümlülükleri sebebiyle elektronik imza uygulamasındaki taraflardan sayılabilecektir[11]. Aşağıda elektronik imza

[11] e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları, Kasım 2005, s. 5

uygulaması kapsamında ortaya çıkan taraflar yine elektronik imza uygulaması esas alınarak oluşturulmuş bir bakış açısı ile incelenecektir.

I. Elektronik Sertifika Hizmet Sağlayıcı

ESHS'lerin, elektronik imza uygulamasındaki esas fonksiyonu, uygulamayı başlatan "imzalayan"ı tanımlamalarıdır. Bilindiği üzere imzalayan kişinin uygulamada imzalayan olarak yer alabilmesi için öncelikle ESHS'ye kimliğini kanıtlaması ve ESHS'den nitelikli elektronik sertifika alması gereklidir[12]. Bu durumda, elektronik imza uygulaması ile sınırlı bir kapsamda düşünüldüğünde imzalayanı var eden ESHS'dir denilebilir. Çünkü imzalayanla ilgili olarak, uygulamanın imzalama ve doğrulama süreçleri için gerekli olan, sadece geçerliliğini sürdüren bir nitelikli elektronik sertifikadır. Bu nitelikli elektronik sertifikanın gerçekten var olan bir şahsa ait olup olmadığı veya içerdiği bilgilerin doğru olup olmadığı otomatik süreçler dahilinde işleyen elektronik imza uygulaması için önemli değildir. Ayrıca bu bilgilerin doğruluğu, genel olarak uygulama tarafından çapraz bilgilerle kontrol edilmez. Bu sebeple elektronik imza uygulamasında dinamik taraf olan imzalayanı tanımlayan hatta var eden ESHS'lerin, elektronik imza uygulamasındaki en önemli taraf olduğu kesindir; dolayısıyla kendilerine ilişkin sorumluluk rejiminin ve regülasyon stratejisinin detaylı bir şekilde yapılandırılması gerekmektedir[13].

Ülkemizde ESHS'lerin hak ve yükümlülükleri 5070 sayılı Elektronik İmza Kanunu, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenmektedir. 5070 sayılı Elektronik İmza Kanunu ile Telekomünikasyon Kurumu konuyla ilgili regülasyon yetkisine sahip olmuştur.

---

[12] Collins. T. DESS Droit de l'Internet - Administration – Entreprises, Aspects techniques et juridiques des infrastructures de gestion de clés publiques**,** septembre 2004, s23

[13] Smedinghoff T.J. , Certification Authority Liability Analysis, Baker & McKenzie, Chicago, s.7

Elektronik İmza Kanunu ve ilgili ikincil düzenlemelere göre ESHS'lerin temel yükümlülükleri şunlardır;

- Yeterli ve yetkin personel istihdamı
- Elektronik sertifika hizmetlerinin sağlanacağı güvenli fiziksel ortamın sağlanması
- Nitelikli elektronik sertifika sağlayacağı kişilerin kimlik tespitinin ve eğer sertifika talep eden kişi isteniyorsa bu kişilerin üçüncü kişiler adına hareket etme yetkisinin ve/veya mesleki ve kişisel bilgilerinin geçerliliğinin tespitinin yapılması
- Oluşturulduğu mecraya göre hem kendi kök sertifikasıyla hem de kullanıcıların sertifikalarıyla bağlı elektronik imza oluşturma verilerinin güvenliğinin ve gizliliğinin sağlanması
- Nitelikli elektronik sertifika talep edilen kişilerin, konunun hukuki ve teknik boyutu hakkında bilgilendirilmesi
- Kayıt tutma ve arşivleme
- Kişisel verilerin korunması
- Nitelikli elektronik sertifika sağladığı kişilerin sertifika iptal ve askıya alma hizmetlerini gerçekleştirmesi
- Sertifika mali sorumluluk sigortası yaptırılması
- Kullanıcılarına sağladığı güvenli elektronik imza oluşturma ve doğrulama araçlarının ve imza oluşturma uygulamalarının ilgili

düzenlemeyle belirlenen standartlara uygun olduğunun tespit edilmesi ve bu durumun taahhüt edilmesi

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen ve ESHS'ler tarafından uyulmak zorunda olan ETSI TS 101 456 ve CWA 14167-1 standartlarında yukarıda belirtilen yükümlülükler detaylı bir şekilde incelenmekte ve bazı farklı yükümlülüklere yer verilmektedir. Bu standartlarda belirtilen yükümlülükler çalışmanın ilgili bölümünde ayrıca incelenecektir.

ESHS'lerin sorumlulukları da 5070 sayılı Elektronik İmza Kanunu'nu ile belirlenmiştir. Kanun'un 13. maddesine göre elektronik sertifika hizmet sağlayıcıların sorumlulukları genel hükümlere belirlenecek ancak elektronik sertifika sağlayıcılar, Elektronik İmza Kanunu ve ilgili ikincil mevzuat hükümlerine aykırı hareket ederek üçüncü kişilere zarar verdikleri takdirde bu zararı tazmin edeceklerdir. Burada ESHS'lerin kusur sorumluluğu bulunmakla beraber ispat yükü zarar tazmini talebinde bulunana değil ESHS'ye yüklenmiştir. Ayrıca söz konusu zararın ESHS'nin istihdam ettiği kişinin davranışlarına dayanması halinde, ESHS bu zarardan da sorumlu olacak ve Borçlar Kanunu'nun 55. maddesinde öngörülen türden bir kurutuluş beyyinesinden faydalanamayacaktır. Bu hüküm ESHS'nin yeterli ve yetkin personel istihdamına ilişkin yükümlülüğünün de sonuçları arasında sayılabilir. Uygulamada ESHS'nin kusursuzluğunu ispat edebilmesi için en önemli etken ilgili yasal düzenlemelere ve bu düzenlemelerde belirtilen standartlara uyduğunu kanıtlaması olacaktır. Söz konusu düzenlemeler ve ilgili standartlar ESHS'ler için öngörülebilir bir sorumluluk ve yükümlülük yapısını oluşturmakta ve objektif sorumluluğu yerine getirmenin kriterlerini oluşturmaktadırlar.

ESHS'nin en önemli yükümlülüğü olan sertifika talebinde bulunan kişinin kimliğini, (talep edilmesi halinde) mesleki ve kişisel bilgilerini, üçüncü kişiler adına hareket etme yetkisini doğrulaması ve kayıt altına almasıyla ilgili sorumluluk, bu

işlemin yapıldığı anla beraber yorumlanmalıdır[14]. ESHS'nin kimlik doğrulama yükümlülüğü sadece bu doğrulamayı yaptığı anda kimlik bilgilerinin geçerliliğini kontrol etmesine dayanır. ESHS'nin sertifikayı sağlamasından sonra sertifika sahibinin kimlik bilgilerinin ve sertifikada yer alıyorsa mesleki ve kişisel bilgilerinin değişmesi ve bu durumu ESHS'ye bildirmemesi ESHS'nin sorumluluğu dışındadır.

ESHS'lerin sorumluluklarını sınırlandırabildikleri tek durum nitelikli elektronik sertifikanın kullanım ve maddi kapsamına ilişkin sınırlamalardır. Elektronik İmza Kanunun 9. maddesine göre bu sınırlamalara ilişkin bilgiler nitelikli elektronik sertifikanın içerisinde yer almalıdır. Sınırlama bilgilerinin sertifika içerisinde ne şekilde yer alacağı, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 5. maddesinde belirtilen ve nitelikli elektronik sertifikaların uyumlu olmak zorunda oldukları ETSI TS 101 862 standardında ayrıntılı olarak belirtilmiştir. Standardın "nitelikli elektronik sertifika ibareleri" (qualified certificate statements) bölümünde, sınırlama bilgileri girilirken, para birimi olarak ISO4217 kodlarının kullanılabileceği ve işlem sınırı için maddi değer aralığının gösterilebileceği belirtilmiştir[15]. TÜBİTAK-UEKAE tarafından nitelikli elektronik sertifika profili ile ilgili olarak yapılan çalışmada da[16] para birimi olarak ISO 4217 kodları altında Türk Lirası için TRL, Yeni Türk Lirası için TRY kodunun kullanılması gerektiği belirtilmiştir.

ETSI TS 101 862 standardında ve TÜBİTAK-UEKAE tarafından yapılan çalışmada, nitelikli elektronik sertifikaların maddi kapsamlarına ilişkin sınırlamaların nasıl yapılacağı belirlenirken, kullanım kapsamlarına ilişkin sınırlamanın ne şekilde yapılacağı belirtilmemiştir. Sertifikanın kullanım kapsamına ilişkin sınırlamanın "anahtar kullanımı eklentisi" (key usage extension) ile belirtilebileceği düşünülse de esasta bu eklenti sertifikanın hangi amaçla kullanılacağını belirtmek içindir. Bilindiği

[14] Sevim T., İstanbul Barosu Staj Eğitim Merkezi, Bireysel Çalışma Raporu, Elektronik İmzanın Hukuksal Boyutları: Mevcut Durum Eksiklikler ve Çözüm Önerileri, İstanbul, Şubat 2005 s.18

[15] ETSI TS 101 862, Qualified Certificate profile, V1.3.3, Valbonna – France, 2006

[16] Soran S., Gülaçtı E., Teknik Rapor: Nitelikli Elektronik Sertifika Profili, TÜBİTAK UEKAE Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Ağustos 2005

üzere elektronik sertifikalar güvenli elektronik imza yaratma fonksiyonları dışında çeşitli güvenlik ve kimlik tanımlama teknolojilerinde de kullanılmaktadırlar. Elektronik sertifika içerisindeki anahtar kullanımı eklentisi; sertifikanın başka bir sertifikayı imzalaması, sertifika iptal listesini imzalaması, dijital imza ve inkar edilemezlik fonksiyonları gibi kullanım alanları için kullanılmaktadır. Nitelikli elektronik sertifikalarda ise, anahtar kullanım eklentisinin sadece, inkar edilemezlik eklentisi tek başına olacak şekilde veya dijital imza eklentisi ile birlikte kullanılması gerekmektedir[17]. Bu sebepten ötürü kullanım kapsamına ilişkin sınırlandırmanın, "anahtar kullanımı eklentisi" ile yapılamayacağı açıktır.

Kanaatimizce, kullanım kapsamına ilişkin sınırlama ESHS tarafından ancak sertifika ilkeleri, imza ilkeleri veya bunlara benzer bir ibare ile belirlenebilecektir. Bunlardan sertifika ilkeleri ve imza ilkeleri dokümanları, tümüyle sertifikanın içerisinde yer almasalar dahi nitelikli elektronik sertifikanın "sertifika ilkeleri eklentisi" (certificate policies extension) içerisinde isim, (URL) ve nesne belirteci (OID) şeklinde referans gösterilmek suretiyle sertifika kapsamına dahil edilirler[18]. Bu durumda ESHS'nin sertifika kullanım kapsamıyla ilgili belirlediği ve sertifika ilkeleri ve/veya imza ilkeleri dokümanlarında yer verdiği sınırlandırmalar (bunların sertifika içerisinde yukarıda belirtilen yöntemlerle referans gösterilmesi halinde), nitelikli elektronik sertifika sahibi için geçerli olacak ve bu sınırlandırmalar ESHS'nin sorumluluk kapsamını belirleyecektir. Burada dikkat edilmesi gereken nokta; sertifikanın kullanım kapsamına ilişkin ESHS sorumluluğuyla ilgili olarak, sertifika ilkeleri ve imza ilkeleri dokümanlarının sözleşme veya tek taraflı irade beyanı nitelikleri dışında değerlendirilmesi gerektiğidir. Elektronik İmza Kanunu'nun 13. maddesine göre;

"Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü

[17] Soran S., Gülaçtı E., Teknik Rapor: Nitelikli Elektronik Sertifika Profili, TÜBİTAK UEKAE Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Ağustos 2005 s. 6

[18] Network Working Group, Internet X.509 RFC 3280 Certificate and Certificate Revocetion List Profile, April 2002

kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir."

Bu doğrultuda sertifika ilkeleri ve imza ilkeleri dokümanları, Elektronik İmza Kanunu kapsamında, teknik ve hukuki yapıları sebebiyle, "sertifikanın içerdiği kullanım ve maddi kapsama ilişkin sınırlamaları" belirleyen dokümanlardır ve Kanun maddesinde geçen diğer "her türlü şart" içerisine girmemektedirler. Sertifika ilkeleri ve imza ilkeleri dışında, kullanım kapsamını belirlemek üzere, sertifikanın içerisinde "sertifika ilkeleri eklentisi" bölümünde sınırlamaya ilişkin ibareler yer alabilir; ancak bu ibareler teknik kısıtlamalar sebebiyle kısa metinlerden oluşmalıdır.

ESHS'ler tarafından sağlaması gereken elektronik sertifika hizmetleri kendi içerisinde kademeli olarak birbirlerinden ayrılmaktadır. ESHS bu hizmetlerin hepsini kendisi sağlayabileceği gibi bu hizmetleri sağlayan kişi ve kurumlarla da çalışabilir. Ancak bu hizmetler ESHS tarafından sağlanmasa dahi ESHS'nin Elektronik İmza Kanunu'nun 13. maddesinden kaynaklanan münhasır sorumluluğu sebebiyle, üçüncü kişiler açısından hizmetlere ilişkin sorumluluk ESHS'de doğacaktır. Böyle bir durumda zarar gören üçüncü kişi zararını tazmin için, zararı doğuran hizmet sağlayıcısına değil ESHS'ye başvuracaktır. ESHS ile ilgili hizmeti sağlayan arasındaki hukuki durum ise aralarındaki sözleşme ve genel ilkeler doğrultusunda yorumlanacak ve çözümlenecektir.

Elektronik sertifika hizmetleri aşağıdaki bileşenlerden oluşmaktadır[19];

- Kayıt Hizmetleri: Sertifika sahibinin kimliğinin ve talep ediliyorsa mesleki ve kişisel bilgilerinin doğrulanması ve kayıt edilmesi

- Sertifika Yayınlama Hizmetleri: Doğrulanan kimlik bilgileri ve diğer bilgiler üzerine sertifikanın yaratılması ve imzalanması

[19] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s.10

- Dağıtım Hizmetleri: Sertifikanın, sertifika ilkeleri ve esaslarının ve diğer ilgili dokümanların, sertifika sahibine ve diğer üçüncü taraflara iletilmesi, bu tarafların erişimi için gerekli teknik alt yapının hazırlanması

- Sertifika İptal Yönetimi Hizmetleri: Sertifika iptal ve askı taleplerinin alınması ve işlenmesi

- Sertifika İptal Bilgisi Yayınlama Hizmetleri: Çevrimiçi sertifika durum protokolü (OCSP) veya sertifika iptal listesi (CRL) gibi teknikler aracılığıyla sertifika durum bilgilerinin ilgili üçüncü taraflara iletilmesi

- Güvenli Elektronik İmza Oluşturma Aracı Dağıtım Hizmetleri: Güvenli elektronik imza oluşturma aracının son kullanıcılara dağıtılması; bu hizmet elektronik imza oluşturma verisinin araç içerisinde oluşturulmasından sonra veya oluşturulmasından önce sağlanabilir.

II. İmzalayan

Elektronik imza uygulamasında, "imzalayan" süreci başlatan dinamik taraftır[20]. İmzalayan, imza uygulamasının özelliklerine göre, imza uygulaması içerisinde çeşitli roller ve sorumluluklar edinebilir. İmza uygulaması, imzalayan kullanıcı tarafından esnekliğe uğratılabilir özellikte ise veya uygulama içerisinde kullanıcıya çeşitli seçenekler sunuyorsa, imzalayanın uygulamaya aktif katılımı artmakta ve buna göre sorumluluk yapısı değişmektedir. Örnek vermek gerekirse, web tabanlı basit bir form doldurma ve bu formu imzalama uygulamasında, imzalayan sadece formu doldurmak ve

[20] Forum of European Supervisory Authorities for Electronic Signatures (FESA), Working Paper on Qualified Certificates for Automatically Signing Systems, October 2004 s. 1

bu form üzerindeki bilgileri imzalamak yetkisine sahiptir. Ancak son kullanıcının daha önceden yarattığı bir dokümanı, harici bir elektronik imza oluşturma yazılımı ile imzalaması ve bu yazılımın içerisinde; imza taahhüdü[21] (signature commitment), imza ilkeleri (signature policy) belirleme gibi seçenekler bulunması halinde, imzalayanın uygulamaya katılımı artacak ve imzalama ile ilgili sorumluluk yapısı değişecektir.

Burada imzalayanın sorumluluk yapısını değiştiren, imza uygulamasında kendisine sunulan seçeneklerdir. Şöyle ki, imza uygulaması, imzalayana imza taahhüdünü belirleme yetkisi veriyorsa, imzalayan belirlediği taahhüde göre imzasıyla sorumlu olacaktır. İmzalayan, imza taahhüdünü, onay, alındı, yaratma gibi farklı amaçlar doğrultusunda belirleyebilir. İmzalayan, taahhüdü belirledikten sonra, imzalı belge ile, belirlediği taahhüt doğrultusunda sorumlu olacaktır. Yani alındı amacıyla belgenin imzalanması, imzalayana belgeyi yaratan ve imzalayan sorumluluğunu getirmez, imzalayan sadece belgeyi teslim almış olduğunu belirtmekte ve belgeyi teslim almış olmakla sorumlu olmaktadır. İmzalayan, imza ilkesi belirleme seçeneğini kullanarak ise imza uygulamasında seçtiği imza ilkelerinin hükümleriyle bağlı olacağını kabul etmekte ve doğrulayanın da imzalı belgeye dayanarak işlem yaptığı takdirde, imzalayanın seçtiği imza ilkeleri hükümleri ile bağlı olacağını belirtmektedir. İmza ilkeleri, yine imza oluşturma yazılımının niteliklerine göre, imzalayan tarafından yaratılabilir veya mevcut imza ilkeleri içerisinden seçilebilir.

İmzalayan, 5070 sayılı Elektronik İmza Kanunu'nun 3. maddesinde "imza sahibi" olarak tanımlanmıştır. Bu tanıma göre imza sahibi; elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir. Güvenli elektronik imza uygulamasına bakıldığında imza sahibi/imzalayan aynı zamanda nitelikli elektronik sertifika sahibi olarak karşımıza çıkmaktadır; zira güvenli elektronik imza uygulamasında, güvenli elektronik imza sadece güvenli elektronik imza oluşturma aracı ve nitelikli elektronik sertifika ile oluşturulabildiği için; imza sahibi/imzalayanın aynı zamanda nitelikli elektronik sertifika sahibi olması da gerekmektedir. Elektronik İmza

[21] ETSI TS, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), V1.6.3, Valbonna – France, 2005 s. 28

Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile nitelikli elektronik sertifika sahibinin yükümlülükleri belirlenmiştir. Bu yükümlülükler yukarıda belirtilen uygulamalı kaynaklı yükümlülüklerin yanında mevzuattan kaynaklanan yükümlülükler olarak ele alınmalıdır. Yönetmeliğin 15. maddesine göre nitelikli elektronik sertifika sahibi/imzalayan;

a) Nitelikli elektronik sertifika almak için gerekli tüm bilgi ve belgeleri eksiksiz ve doğru olarak sağlamakla,

b) ESHS'ye vermiş olduğu bilgilerde değişiklik meydana gelmesi halinde ESHS'yi derhal bilgilendirmekle,

c) İmza oluşturma verisini kendisi üretmesi durumunda Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenen algoritmaları ve parametreleri kullanmakla,

d) İmza oluşturma ve doğrulama verilerini sadece elektronik imza oluşturma ve doğrulama amaçlı olarak ve nitelikli elektronik sertifikanın içerdiği kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanmakla,

e) İmza oluşturma verisini başkalarına kullandırmamakla ve bu konuda gerekli tedbirleri almakla,

f) İmza oluşturma verisinin gizliliğinden veya güvenliğinden şüphe etmesi durumunda ESHS'yi derhal bilgilendirmekle,

g) Güvenli elektronik imza oluşturma aracını kullanmakla,

h) İmza oluşturma ve doğrulama verilerinin ESHS'ye ait olmayan yerlerde ve araçlarla üretilmesi durumunda gerekli güvenliği sağlamakla,

i) İmza oluşturma aracının veya erişim verisinin kaybolması, çalınması, güvenilirliğinden şüphe edilmesi durumunda ESHS'yi derhal bilgilendirmekle,

yükümlüdür.

III. Doğrulayan/Güvenen Üçüncü Taraf

Elektronik imza uygulamasında doğrulayan, imzalı belgeye güvenerek işlem yapan ve imzalı belgeyi alan taraftır[22]. Elektronik imza uygulamasına göre doğrulayan bir gerçek kişi olabileceği gibi aynı zamanda bir sunucu (server) da olabilir. Burada dikkat edilmesi gereken nokta doğrulama işlemini, ister gerçek kişi gerçekleştirsin ister bir sunucu gerçekleştirsin, doğrulamaya ilişkin sonuçların imzalı belgenin gönderildiği şahsa ilişkin olarak doğacak olmasıdır. Bu durum elle (manuel) olarak doğrulamanın yapıldığı anlardan çok bir güvenli elektronik imza doğrulama aracı kullanıldığı zamanlarda ortaya çıkmaktadır. Güvenli elektronik imza doğrulama aracı, Elektronik İmza Kanunu'nun 7. maddesinde şu şekilde tanımlanmıştır;

Güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

[22] Sabo J.T., Dzambasow Y.A., PKI Policy White Paper, PKI Forum, March 2001, s.3

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

imza doğrulama araçlarıdır.

Görüldüğü üzere Kanun'da güvenli elektronik imza doğrulama araçlarına ilişkin nitelikler teknoloji - nötr bir şekilde tanımlanmıştır. Uygulamaya bakıldığında ise, güvenli elektronik imza doğrulama araçlarının sunucu veya kullanıcı tabanlı yazılımlar olduğu görülmektedir[23]. Güvenli elektronik imza doğrulama aracı, çoğu zaman yürüttüğü teknik işlemleri önyüzde kullanıcıya göstermeden çalışmaktadır; ancak mevzuat ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenen CWA 14171 standardına göre bazı fonksiyonel arayüzlerin ve bilgilerin kullanıcıya gösterilmesi zorunludur[24].

Doğrulayan, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te üçünc kişiler olarak tanımlanmıştır. Yönetmeliğin 16. maddesinde

Üçüncü kişiler;

a) Sertifikanın "nitelikli elektronik sertifika" olup olmadığını kontrol etmekle,

[23] CEN Workshop Agreement, CWA 14171 General guidelines for electronic signature verification, may 2004 s. 42

[24] CEN Workshop Agreement, CWA 14171 General guidelines for electronic signature verification, may 2004 s. 28

b) Nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla,

c) Nitelikli elektronik sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmekle,

yükümlüdür.

Maddenin b bendine göre, doğrulayan, imzalı belgeyi aldıktan sonra nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla yükümlüdür. B bendi, maddenin bütünü doğrultusunda okunduğunda doğrulayanın, güvenli elektronik imza doğrulama aracı kullanmasına rağmen, nitelikli elektronik sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmekle ve sertifikanın "nitelikli elektronik sertifika" olup olmadığını kontrol etmekle ilgili yükümlülüğünün devam ettiği söylenebilir. Ancak CWA 14171 standardına tam uyumluluk sağlayan bir güvenli elektronik imza doğrulama aracı, yukarıda belirtilen ek yükümlülüklere ilişkin kontrolleri de yerine getirmektedir. Bu sebeple CWA 14171'e tam uyumluluk sağlayan ve ilgili yükümlülüklere ilişkin kontrolleri yerine getirmekle ilgili niteliklere haiz olan güvenli elektronik imza doğrulama aracını kullanan kullanıcılar, sadece aracı kullanmakla Yönetmelik'le belirlenen yükümlülüklerini yerine getirmiş sayılmalıdırlar.

Burada dikkat edilmesi gereken başka bir husus ise, güvenli elektronik imza oluşturma aracının aksine güvenli elektronik imza doğrulama aracının, kullanıcının münhasır kontrolü altında bulunma zorunluluğunun bulunmayışıdır. Bu durum sunucu tabanlı güvenli elektronik imza doğrulama araçlarının ve güvenli elektronik imza doğrulama hizmetlerinin ortaya çıkmasına sebebiyet verecektir. Ancak güvenli elektronik imza doğrulama hizmetlerini ESHS'ler tarafından verilen sertifika iptal bilgisi yayınlama hizmetlerinden ayırmak gerekmektedir. Güvenli elektronik imza doğrulama hizmetleri, bir güvenli elektronik imza doğrulama aracı ile doğrulama işlemlerinin kullanıcı adına yapılması işlemidir. Güvenli elektronik imza doğrulama hizmetleri, bu işlemi ESHS tarafından verilen sertifika iptal bilgisi yayınlama

hizmetlerini kullanarak gerçekleştirir. Burada güvenli elektronik imza doğrulama hizmetlerini kimin verebileceği sorusu sorulabilir; zira güvenli elektronik imza doğrulama hizmeti belirli bilgi güvenliği kurallarına uygun olarak yerine getirilmeli ve kullanılan doğrulama aracının gerekli niteliklere sahip olduğunun kanıtlanması gereklidir.

Bu durumda en doğru yol Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtildiği üzere, güvenli elektronik imza doğrulama aracının CWA 14171 uygunluğunun kanıtlanmasıdır. Tebliğ'de ilgili standart ESHS'lerin sağlamış olduğu güvenli elektronik imza doğrulama araçları için zorunlu olarak belirlenmiştir. Ancak işleyişin güvenliği ve sorumluluğun belirlenmesi için, kanaatimizce, bu standart tüm güvenli elektronik imza doğrulama araçları için kullanılmalıdır. Burada bir diğer sorun güvenli elektronik imza doğrulama aracının CWA 14171'e uygunluğunu kimin denetleyeceğidir. Elektronik İmza Kanunu ve ilgili ikincil mevzuatta, güvenli elektronik imza araçları ile ilgili akreditasyon ve standart uyumluluk kontrolü için hiçbir yetkili kurum ve akreditasyon şeması belirlenmemiştir. Bu durum uygulamada ciddi problemlere yol açmakta ve pazarda belirsizliklere sebebiyet vermektedir.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ve daha sonra çıkan Telekomünikasyon Kurumu Kararları ile eğer araçlar ESHS tarafından sağlanıyorlarsa, araçların standartlara uygunluğunun, ESHS tarafından taahhüt edilmesi gerektiği belirtilmiştir. Burada regülatörün amacı, piyasanın kendi iç dinamikleri içerisinde kendi kurallarını belirlemesi ve akreditasyon ile ilgili bir nevi self-regulation yapısının kurulmasıdır. Bu durum uygulamada araç sağlayıcıların, ESHS'ler ile çalışmasına ve yazılımlarının ilgili standartlara uyumluluğu konusunda ESHS'lerden taahhüt almasına yol açmaktadır. Böylece Kanun ile yetkilendirilen güvenilir üçüncü parti ESHS'ler, araçların standartlara uyumluluğu konusunda da sorumluluk sahibi durumuna gelmektedirler.

IV. Uygulama Sağlayıcı, Politika/İlke Belirleyici

Elektronik imza uygulamasında, uygulama sağlayıcı elektronik imza uygulamasını oluşturan ve imzalayanın (uygulamanın çeşidine göre doğrulayanın) kullanımına sunan taraftır. Burada bahsedilen uygulama, imzalayanın elektronik imza atmasını sağlayan yazılım/ortam'dır. Şunu belirtmek gerekir ki; burada bahsedilen uygulama, güvenli elektronik imza oluşturma aracı değildir. Güvenli elektronik imza oluşturma aracı, elektronik imza uygulamasının bir parçası olmakla birlikte, uygulama/yazılım güvenli elektronik imza aracının da yardımıyla elektronik imzanın oluşturulmasını sağlar[25]. Bu doğrultuda elektronik imzanın atılmasını sağlayan yazılım ve ara yüzler, Elektronik İmza Kanunu ve ilgili ikincil mevzuattaki güvenli elektronik imza oluşturma aracının tanımlarına dahil olmayıp burada belirtilen nitelikler haiz olmak zorunda değildirler. Bu uygulamalar/yazılımlar, ESHS'ler tarafından sağlandığında, Telekomünikasyon Kurulu'nun 01.06.2006 tarihli Kararı doğrultusunda, uygulamaların CWA 14170 standardına uyumluluğunun sağlanması gerekmektedir.

Elektronik imza uygulamaları, bireysel ve topluluk uygulamalarına ilişkin çözümler olarak ikiye ayrılabilir. Bireysel elektronik imza uygulamaları, sadece son kullanıcı tarafından kullanılabilen, son kullanıcının kişisel aracına/terminaline (kişisel bilgisayar, cep telefonu, v.b.) yüklenen ve burada çalıştırılan yazılımlardır. Topluluk uygulamaları ise, imzalama işleminin web sunucusu gibi pek çok kullanıcının kullanımıma açık olan ve imzalayanın imzalama işlemini gerçekleştirmek için "erişmek" zorunda olduğu uygulamalardır. Ülkemizde mevcut tek topluluk uygulaması, Dış Ticaret Müsteşarlığı tarafından geliştirilen Dahili İşleme Rejimi Projesidir[26].

Elektronik imza uygulama sağlayıcısı, elektronik imza uygulamasının, güvenliğini sağlamak ve bunu sürdürmekle yükümlüdür. Bu noktada, bireysel elektronik imza uygulaması ile topluluk uygulamaları arasında bir farklılık olduğu

[25] CEN Workshop Agreement, CWA 14170 Security requirements for signature creation applications, May 2004 s.14

[26] https://edtm.dtm.gov.tr/basvuru/giris.jsp

düşünülebilir; şöyle ki bireysel elektronik imza uygulamasının sağlayıcısı, kullanıcının söz konusu uygulamayı/yazılımı aldığı yazılım firması olacaktır. Ancak topluluk uygulamalarında, bu sorumluluk uygulamayı işleten tarafa ait olacaktır ve bu taraf büyük ihtimalle yazılımı geliştiren firma değil yazılımı kullanan ve topluluk uygulamasını geliştiren kurum/kişi olacaktır. Böyle bir durumda uygulama sağlayıcısı, elektronik imza uygulamasının işleyişinden veya güvenliğinden dolayı, imzalayanın bir zarara uğraması halinde bu zararı tazminle yükümlü olacaktır. Ancak her halükarda uygulama sağlayıcısının yazılım geliştirici firmaya rücu hakkından bahsedilebilir. Uygulamanın ESHS tarafından sağlandığı durumlar ise yukarıdaki durumlara istisna olarak ortaya çıkmaktadır, böyle bir durumda uygulama ister bireysel ister topluluk uygulaması olsun sorumluluk, CWA 14170 standardına zorunlu uyumluluğu sağlamak zorunda olan ESHS'ye ait olacaktır. Ancak zarar standarda uyumluluğun kapsamı dışında gerçekleşirse, zararın ortaya çıkmasına sebebiyet veren fiili gerçekleştiren veya ihmalde bulunan zararı tazminle yükümlü olacaktır.

Elektronik imza uygulamasının güvenliği veya işleyişi ile ilgili bir sorun ortaya çıktığında, uygulama sağlayıcının kusurundan bahsedebilmek için uygulama sağlayıcının objektif sorumluluğunu yerine getirip getirmediği tespit edilmelidir. Böyle bir durumda, uygulama sağlayıcının objektif sorumluluğunu yerine getirip getirmediğinin tespiti ilk bakışta oldukça zor olacaktır; zira uygulama sağlayıcının objektif sorumluluğunu yerine getirmesi için yapması gerekenler temel bilgi güvenliği kriterleri dışında çok da belirlenebilir değildir; çünkü mevzuatta elektronik imza uygulama sağlayıcının hak ve yükümlülüklerine ilişkin hükümler bulunmamaktadır. Burada Elektronik İmza Kanunu'nun 8. maddesi uygulamamaktadır, çünkü 8. madde metni içerisinde her ne kadar elektronik imza ile ilgili hizmetleri sağlayanlar da ESHS olarak kabul edilse de madde metni bütünü ile okunduğunda ve konuyla ilgili uluslararası standartlar göz önüne alındığında elektronik imza uygulaması sağlayanların elektronik sertifika hizmet sağlayıcısı olmadıkları açıklıkla ortaya çıkmaktadır. Bu sebeple, elektronik imza uygulama sağlayıcılarının, elektronik sertifika hizmet sağlayıcıların tabi oldukları hak ve yükümlülüklere tabi olmaları mümkün değildir.

Elektronik imza uygulama sağlayıcının objektif sorumluluğuna ilişkin kriterin belirlenmesi için en önemli argüman Telekomünikasyon Kurulu'nun 01.06.2006 tarihli Kararı ile belirlenen CWA 14170 standardına uyumluluğun sağlanması durumudur. Kurul Kararı'nda, CWA 14170 standardına uyumluluğun, ESHS'ler tarafından sağlanan elektronik imza uygulamaları için zorunlu olduğu belirtilse de, standart CEN tarafından aslında tüm elektronik imza uygulamaları için belirlenmiştir. Bu durum ülkemizde CWA 14170'in uygulanması bakımından iki sonuç ortaya çıkarmaktadır; ihtiyari uyumluluk ve zorunlu uyumluluk. CWA 14170, elektronik imza uygulaması sağlayan ESHS'ler için bir zorunluluk iken, diğer elektronik imza uygulama sağlayıcılar için ihtiyari bir husus haline gelmektedir. Bu ihtiyari uyumluluk, elektronik imza uygulama sağlayıcılara, mahkeme önünde objektif sorumluluklarını yerine getirdiklerini kanıtlamada yardımcı olacaktır.

Burada bir diğer sorun, elektronik imza uygulama sağlayıcının CWA 14170 standardına uyum sağladığını nasıl kanıtlayacağıdır. Daha önce de bahsedildiği gibi, ülkemizde söz konusu CEN ve ETSI standartlarına ilişkin akreditasyon sağlayan resmi bir kurum bulunmamaktadır. Mevzuata göre ise ESHS'ler sağlamış bulundukları elektronik imza uygulamaları ve elektronik imza doğrulama araçları için uyumluluk taahhüdünde bulunmaktadırlar. Bu durum uygulamada, elektronik imza doğrulama araçları için, elektronik imza doğrulama aracı kullanıcısının, bu aracı ESHS'den temin etmesi veya doğrulama aracı yazılımcısının kullanıcılarına ESHS üzerinden yazılım sağlaması ve böylece söz konusu araçlara ilişkin bir nevi akreditasyon olan uyumluluk taahhüdünün gerçekleştirilmesi olarak karşımıza çıkmaktadır. Aynı durum 01.06.2006 tarihli Telekomünikasyon Kururlu Kararı'nın yayımlanmasından sonra büyük ihtimalle elektronik imza uygulamaları ile ilgili olarak da ortaya çıkacaktır. Söz konusu taahhüt sistemi ile elektronik imza uygulaması sağlayıcıları hem uygulamalarının standarda uyumlu olduğunu kanıtlayabilmekte hem de sorumluluk konusunda ilk muhatap olarak ESHS'nin ortaya çıkmasını sağlamaktadırlar. Ancak bu yolu tercih etmeyen elektronik imza uygulama sağlayıcılar, CWA 14170 uyumluluğu için yine CEN tarafından yayınlanan ve ilgili standarda uyumluluğun ne şekilde ortaya konulacağını açıklayan CWA 14172-4 belgesi doğrultusunda uyumluluk bildirimini gerçekleştirebilirler. CWA 14172-4'de belirtildiği üzere, CWA 14170 uyumluluğu için, elektronik imza

uygulamasını geliştiren firmanın ve bu uygulamayı işleten operatörün yine belgede belirtilen esaslar doğrultusunda uyumluluk bildiriminde bulunması yeterli olacaktır[27].

Elektronik imza uygulamasında, uygulama sağlayıcı, uygulamaya ilişkin elektronik sertifika kullanma prensiplerini ve/veya elektronik imza kullanımına ilişkin kuralları belirleyebilir. Bu durumlarda elektronik imza uygulama sağlayıcı, aynı zamanda politika/ilke belirleyici konuma da gelecektir. Elektronik imza uygulamasında sertifikanın kullanım kurallarına ilişkin olarak, ESHS tarafından belirlenen sertifika ilkeleri ve sertifika uygulama esasları dışında bir kural belirlenmek istenirse, bu kurallar elektronik imza uygulaması sağlayıcısı tarafından sertifika ilkeleri dokümanı ile belirlenebilir. Bu sertifika ilkeleri, kullanılan sertifikaların bağlı olduğu sertifika ilkeleri ve sertifika uygulama esasları dokümanları ile uyumlu olmak zorundadır. Genel kanının aksine, sertifika ilkeleri dokümanları sadece ESHS'ler tarafından yayınlanmayıp, herhangi bir elektronik imza uygulamasında kullanılmak üzere uygulama sağlayıcı veya ilgili kurum veya kişi tarafından yaratılabilir[28]. Bu konu sertifika ilkeleri ile ilgili bölümde detaylı olarak incelenecektir.

Elektronik imza uygulama sağlayıcı, uygulamaya özel sertifika kullanım koşullarını değil imza kullanım kurallarını belirlemek isterse imza ilkeleri dokümanını yayınlamalıdır. İmza ilkeleri dokümanı, belirtilen uygulama içerisinde elektronik imzanın kullanım amaçlarını, elektronik imza oluşturma ve doğrulama prosedürlerini belirleyen dokümandır. Bu konu da imza ilkeleri ile ilgili bölümde detaylı olarak anlatılacaktır.

Elektronik imza uygulama sağlayıcı, sertifika ilkeleri veya imza ilkeleri yayınlaması durumunda, bu ilkelerin kullanıcılar tarafından erişilebilir bir ortamda tutulmasından ve ilgili mevzuattaki zaman aşımı süreleriyle uyumlu bir süre boyunca

[27] CEN Workshop Agreement, CWA 14172-4 EESSI Conformity Assessment Guidance - Part 4: Signaturecreation applications and general guidelines for electronic signature verification, March 2004 s. 6-7

[28] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s.9

saklanmasından sorumludur. İmzalayan veya doğrulayan, elektronik imza uygulamasını kullanarak imzalama ve/veya doğrulama işlemlerini gerçekleştiriyorlarsa, bu işlemler sırasında imza ilkelerine veya sertifika ilkelerine doğrudan ulaşabiliyor olmalıdırlar. Uygulama aynı zamanda, imzalayana ve/veya doğrulayana, imzalama ve/veya doğrulama işleminden önce ilgili sertifika ilkeleri ve/veya imza ilkeleri dokümanları altında işlem yaptığını göstermeli ve bu dokümanlara doğrudan erişimi sağlamalıdır. Elektronik imza uygulaması, mümkünse elektronik imza verisi içerisinde, ETSI TS 101733 ve ETSI TS 101 933'de belirtildiği gibi, ilgili sertifika ilkeleri ve/veya imza ilkeleri dokümanlarına ait referanslara yer vermelidir[29]. Eğer bu gereklilikler yerine getirilmezse, elektronik imza uygulama sağlayıcı, imzalayanın veya doğrulayanın ilgili imza ve sertifika ilkeleriyle bağlı olduğunu iddia edemeyecek, imzalayan veya doğrulayan sadece ESHS tarafından yayınlanan imza ilkeleri ve sertifika ilkeleri ile bağlı olacaktır.

V. Araç Sağlayıcılar

Elektronik imza uygulamasında, araç sağlayıcılar, güvenli elektronik imza oluşturma ve doğrulama araçlarını, son kullanıcılara ve ESHS'lere sağlayan donanım üreticileri ve satıcılardır. Bilindiği üzere ülkemizde elektronik imza oluşturma aracı üreticisi bulunmadığı için bütün elektronik imza oluşturma araçları ithalatçı firmalar tarafından sağlanmaktadır. Bu durum, uygulamada elektronik imza oluşturma araçlarına ilişkin uygunluk sertifikalarının ithalatçı firmalar tarafından temin edilmesi sonucunu doğurmaktadır[30]. Bilindiği üzere, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 8. maddesine göre, elektronik imza oluşturma araçları, CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL 4+ seviyesinde olmalıdır. Uygulamada güvenli elektronik imza

[29] ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), V1.6.3, Valbonna – France, 2005 s. 15

[30] Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, İstanbul, Temmuz 2004

oluşturma araçlarının EAL 4+ uygunluk belgeleri Telekomünikasyon Kurumu'na verilmektedir.

Elektronik imza oluşturma araçlarının uygunluk belgeleri için, hem aracın çipine (crypto processor) hem de işletim sistemine ait olmak üzere iki adet uygunluk belgesi veya aynı belge içerisinde her iki konunun birden kapsanması durumunu gerekli görülmektedir[31]. Ancak, ne Telekomünikasyon Kurumu ne de ESHS'ler, EAL 4+ seviyesine sahip elektronik imza oluşturma araçlarını deklare etmedikleri için kamuoyunda bu konuda bilgisizlik bulunmaktadır. Güvenli elektronik imzanın oluşturulması için güvenli elektronik imza oluşturma aracı ve nitelikli elektronik sertifika zorunlu unsurlar olmasına ve ESHS'lerin kamuoyuna açıklanmasına rağmen, güvenli elektronik imza oluşturma araçlarına ilişkin bu belirsizlik, güvenli elektronik imza altyapısının oluşturulmasına ve kullanıma ilişkin problemlerin ortaya çıkmasına sebebiyet verebilecektir.

[31] Déler-Castro G., Cruellas-Ibarz J., Electronic Signature Functionality and Security Requirements, UPGRADE Vol. V, No. 3, June 2004 s. 23

İKİNCİ BÖLÜM

ELEKTRONİK İMZA UYGULAMASINDA KULLANILAN DOKÜMANLAR

A. SÖZLEŞMELER

Elektronik imza uygulamasında kullanılan sözleşmeler tarafları açısından, ESHS ile kullanıcılar arasında yapılan sözleşmeler, ESHS ile hizmet sağlayıcılar arasında yapılan sözleşmeler ve ESHS'ler arasında yapılan sözleşmeler şeklinde ayrılabilir. Elektronik imza uygulamasında kullanılan sözleşmeler genel hükümlere tabi olmakla birlikte, Elektronik İmza Kanunu, ilgili ikincil düzenlemeler ve bu düzenlemelerde belirtilen uluslararası standartlara uygunluk göstermek zorundadırlar. Ayrıca Telekomünikasyon Kurumu'na yapılan bildirim esasları doğrultusunda, ESHS'lerin elektronik imza uygulaması ile ilgili sözleşmelerinin Kurum'a verilmesi ve Kurum tarafından uygun bulunması gerekmektedir.

04.02.2006 Tarih'li Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik'le, son kullanıcılarla yapılacak olan sözleşmelerin, taahhütler ile de yapılabilmesi öngörülmüştür. Kanaatimizce bu düzenleme, doğru değildir; zira son kullanıcı ile ESHS arasında yapılan sözleşmede her iki tarafın karşılıklı taahhütlerini içeren bir metine ihtiyaç vardır. Taahhütname ise, sertifika kullanıcısı olmak isteyen şahsın, ESHS'ye karşı tek taraflı taahhütlerini içermektedir. Yönetmelik değişikliği yapılmadan önce Telekomünikasyon Kurumu bünyesinde yapılan tartışmalarda, ESHS'lerin yükümlülüklerinin mevzuatla belirlenmiş olması ve mevzuatın emredici olması sebebi ile ayrıca sözleşmeye gerek olmadığı, sertifika talep eden kişiden tek taraflı taahhüt alınmasının yeterli olacağı şeklinde fikirler öne sürülmüştür. Ancak öncelikle şunu

belirtmek isteriz ki, ESHS'ler gibi, sertifika kullanıcı olmak isteyen şahıslara ve sertifika sahiplerine ilişkin yükümlülükler de aynı şekilde emredici bir biçimde mevzuatta yer almaktadır. Bu sebeple ESHS'lerin yükümlülüklerinin mevzuatta yer alması, tek taraflı bir hukuki metin ortaya koymak için yeterli değildir. Ayrıca ESHS ile sertifika sahibi olmak isteyen şahıs arasında kurulan ilişki bir alım-satım ve devamında hizmet ilişkisidir. Bu sebeple bu ilişki sadece Elektronik İmza Kanunu kapsamında düşünülemez. Bu ilişki aynı zamanda Borçlar Kanunu (Ticaret Kanunu) ve Tüketicinin Korunması hakkında Kanun'a da tabi olacaktır.

Mevcut ESHS'lerin iş modelleri göz önüne alındığında, elektronik sertifikaya ilişkin hizmetlerin (nitelikli elektronik sertifika sağlanması, zaman damgası hizmetleri) ve güvenli elektronik imza oluşturma aracının birlikte ve son kullanıcı ile yüz yüze irtibat kurulmadan sağlandığı görülmektedir. Bu noktada elektronik sertifika sağlanmasının, bir satış akdi mi yoksa bir hizmet sağlama akdi mi olduğu tartışılabilir. Elektronik sertifika ilk bakışta, sertifikanın fiziken son kullanıcıya teslimi olarak gözükse ve satım akdine benzese bile, ESHS tarafından sağlanan esas hizmet, son kullanıcının sertifikasının ESHS sertifikası ile imzalanması, sertifikanın geçerlilik süresi boyunca, sertifika durum kaydı ve iptal hizmetlerinin sağlanmasıdır. Ayrıca ESHS tarafından sağlanan sertifika, son kullanıcı tarafından silinse bile, her zaman ESHS'nin bilgi deposundan indirilebilir. Son kullanıcı sertifikası, sadece son kullanıcının kullanımına münhasır bir menkul değildir. Sertifika üçüncü kişiler tarafından ESHS'nin bilgi deposundan indirilebilir. Aslında sertifika bu noktada ESHS tarafından sağlanan hizmetlerin kullanılabilmesi için bir araçtır. Bu sebeplerle ESHS tarafından sağlanan sertifika hizmetlerine ilişkin son kullanıcı ile yapılan sözleşme bir hizmet sağlama sözleşmesidir. Ancak bu sözleşme, nitelikli elektronik sertifikaların belirli özellikleri sebebiyle bazı ek özellikler taşımaktadır. Yukarıda belirtildiği gibi, nitelikli elektronik sertifikalar, kullanıcıya ait menkuller olmamakla birlikte, yaratılmaları ESHS'ler için bir maliyet getirmekte ve yaratıldıktan sonra başkaları tarafından kullanılamamaktadır. Bu özellikleri sayesinde bazı noktalarda hizmet sağlama sözleşmelerinden farklılık göstermektedirler. Güvenli elektronik imza oluşturma aracın temin edilmesi ise bir satış sözleşmesidir.

Yukarıda bahsedildiği gibi ESHS'lerin mevcut iş modelleri, söz konusu sertifika hizmetlerinin uzaktan satışına ilişkindir. Yani son kullanıcının ESHS'nin yerine gelip burada sertifika alması mevcut modeller içerisinde az rastlanan bir durumdur. Genelde başvurular, noter aracılığı ile veya internet üzerinden yapılmaktadır. Bu durumda son kullanıcılar ile yapılan sözleşmeler Tüketicinin Korunması Hakkında Kanun kapsamında "mesafeli sözleşme" olarak değerlendirilmelidir. Ancak, sertifika talebinde bulunan kişinin, ESHS'nin kendi yerine gelerek (burada kayıt birimleri – registration authority- de ESHS'nin kendi yeri olarak kabul edilmelidir) sertifika talebinde bulunması halinde, bu durum mesafeli sözleşmelerin kapsamına girmeyebilir. Ancak bu durumda sertifika talebinde bulunana kişiye, sözleşme imzalanmadan önce nitelikli elektronik sertifikalar ve güvenli elektronik sertifika ile ilgili gerekli tüm hukuki ve teknik bilgi verilmeli; sertifika talebinde bulunan kişi güvenli elektronik imza oluşturma aracını inceleyebilmeli ve aracın teknik özellikleri ve kullanımı hakkında kendisine yeterli bilgi verilmelidir.

Tüketicinin Korunması Hakkında Kanun'un 9/a maddesi mesafeli sözleşmeler ilişkindir. Madde metni şu şekildedir;

"Mesafeli sözleşmeler; yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelerdir.

Mesafeli satış sözleşmesinin akdinden önce, ayrıntıları Bakanlıkça çıkarılacak tebliğle belirlenecek bilgilerin tüketiciye verilmesi zorunludur. Tüketici, bu bilgileri edindiğini yazılı olarak teyit etmedikçe sözleşme akdedilemez. Elektronik ortamda yapılan sözleşmelerde teyid işlemi, yine elektronik ortamda yapılır.

Satıcı ve sağlayıcı, tüketicinin siparişi kendisine ulaştığı andan itibaren otuz gün içerisinde edimini yerine getirir. Bu süre, tüketiciye daha önceden yazılı olarak bildirilmek koşuluyla en fazla on gün uzatılabilir.

Satıcı veya sağlayıcı elektronik ortamda tüketiciye teslim edilen gayri maddi malların veya sunulan hizmetlerin teslimatının ayıpsız olarak yapıldığını ispatla yükümlüdür.

Cayma hakkı süresince sözleşmeye konu olan mal veya hizmet karşılığında tüketiciden herhangi bir isim altında ödeme yapmasının veya borç altına sokan herhangi bir belge vermesinin istenemeyeceğine ilişkin hükümler dışında kapıdan satışlara ilişkin hükümler mesafeli sözleşmelere de uygulanır.

Satıcı veya sağlayıcı cayma bildiriminin kendisine ulaştığı tarihten itibaren on gün içinde almış olduğu bedeli, kıymetli evrakı ve tüketiciyi bu hukuki işlemden dolayı borç altına sokan her türlü belgeyi iade etmek ve yirmi gün içerisinde de malı geri almakla yükümlüdür."

Görüldüğü üzere, nitelikli elektronik sertifika satışı için son kullanıcılar ile yapılan sözleşme ve hukuki ilişki, maddenin birinci bendinde yapılan tanıma uymaktadır. Maddenin ikinci bendine göre, sözleşmenin imzalanmasından önce, tüketiciye Sanayi ve Ticaret Bakanlığı'nca bir Tebliğ ile belirlenecek olan bilgilerin verilmesi gerekmektedir. Sanayi ve Ticaret Bakanlığı söz konusu tebliğin yerine 13/06/2003 tarihli Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmeliği yayınlamıştır. Yönetmeliğin 5. maddesine göre aşağıdaki bilgilerin, sözleşme akdedilmeden önce tüketiciye verilmesi zorunludur;

- Satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,

- Sözleşme konusu mal ya da hizmetin temel özellikleri,

- Sözleşme konusu mal ya da hizmetin tüm vergiler dahil satış fiyatı,

- Satıcı veya sağlayıcının fiyat dahil tüm vaatlerinin geçerlilik süresi,

- Tüketicinin ödemelerinin nasıl yapılacağına dair bilgiler,

- Teslimat ve ifanın nasıl yapılacağına ve varsa buna ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,

- Cayma hakkı ve bu hakkın nasıl kullanılacağına dair bilgiler,

- Tüketiciye bir maliyeti varsa kullanılan iletişim yollarının ücreti,

- Sözleşme konusu mal ya da hizmetin, teslim ve ifa tarihlerine ilişkin program,

- Tüketicinin talep ve şikayetlerini iletebileceği satıcı veya sağlayıcının açık adres, telefon ve varsa diğer erişim bilgileri.

Yönetmeliğin 6. maddesinde ise, Kanunun 9/A maddesinde olduğu gibi, bu bilgilerin alındığının sözleşme akdedilmeden önce tüketici tarafından onaylanması gerektiği belirtilmektedir. Tüketici bu onayı, elektronik ortamda yine elektronik olarak yapabilmektedir; ayrıca Yönetmeliğe göre her halükarda onay işlemi sertifika ve güvenli elektronik imza oluşturma aracı tüketiciye ulaşmadan yapılmalıdır. Uygulamada bu durum, internet üzerinden yapılan başvurularda, başvurudan önce gerekli bilgilerin gösterilmesi ve elektronik olarak onaylanması; diğer yollarla yapılan ve mesafeli sözleşme kapsamına giren başvurularda ise güvenli elektronik imza oluşturma aracının teslimatından ve sözleşmenin imzalatılmasından önce yapılmalıdır.

Yönetmeliğin 7. maddesine göre, nitelikli elektronik sertifika ve güvenli elektronik imza oluşturma aracının sağlanmasına ilişkin sözleşmelerde en azından aşağıdaki hükümler bulunmalıdır;

- Tüketicinin, satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
- Sözleşmenin düzenlendiği tarih,
- Malın veya hizmetin teslim veya ifa tarihi ve şekli,
- Teslimat ve ifaya ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
- Sözleşme konusu malın veya hizmetin cinsi veya türü, miktarı ve varsa marka ve modeli,
- Malın veya hizmetin Türk Lirası olarak vergiler dahil peşin satış fiyatı,
- Vadeye göre faiz ile birlikte ödenecek Türk Lirası olarak toplam satış fiyatı,
- Faiz miktarı, faizin hesaplandığı yıllık oran ve sözleşmede belirtilen faiz oranının yüzde otuz fazlasını geçmemek üzere gecikme faizi oranı,
- Peşinat tutarı,
- Ödeme planı,
- Borçlunun temerrüde düşmesinin hukuki sonuçları,

yer alır.

Yönetmeliğin 9. maddesinde cayma hakkından bahsedilmektedir. Cayma hakkı tüketicinin malı aldığı veya kendisine sağlanan hizmetin başladığı tarihten itibaren yedi

gün içerisinde hiçbir hukuki ve cezai sorumluluk üstlenmeksizin ve hiçbir gerekçe göstermeksizin malı veya hizmeti reddetme hakkıdır. Bu durumda nitelikli elektronik sertifika veya güvenli elektronik imza oluşturma aracını, mesafeli sözleşme ile alan bir tüketicinin cayma hakkını kullanması halinde bu mal ve hizmetleri geri verme hakkı bulunmaktadır. Ancak burada nitelikli elektronik sertifikanın özelliklerinden dolayı cayma hakkının kullanmasına ilişkin bazı istisnaların oluşabileceği düşünülebilir. Yönetmeliğin 8. maddesinin ikinci fıkrasına göre *"Elektronik ortamda anında ifa edilen hizmetler ve tüketiciye anında teslim edilen mallara ilişkin sözleşmeler cayma hakkı ve kullanımına ilişkin hükümlere tabi değildir*".

Madde metni doğrultusunda, nitelikli elektronik sertifika hizmetlerinin anında ifa edilen hizmetlerden olup olmadığı tartışılabilir; ancak nitelikli elektronik sertifikaya ilişkin hizmetlerin anında başlayabilecek olmasına karşın sertifikanın geçerlilik süresi boyunca devam edecek yapıda olması, nitelikli elektronik sertifika hizmetleri bu hüküm altında yorumlamayı engeller. Aynı maddenin dördüncü fıkrasına göre ise *"tüketici, niteliği itibariyle iade edilemeyecek, hızla bozulma veya son kullanma tarihi geçme ihtimali olan mallar söz konusu olduğunda cayma hakkını kullanamaz."* Bu hüküm doğrultusunda nitelikli elektronik sertifika hizmetleri de nitelikleri dolayısı ile cayma hakkı kapsamına girmeyecek ürünlerden sayılabilir. Burada dikkat edilmesi gereken konu, yukarıda da belirtildiği gibi nitelikli elektronik sertifika satışının bir hizmet sağlama sözleşmesi olmasına rağmen farklı özellikler taşımasıdır. Daha önce de bahsedildiği gibi nitelikli elektronik sertifika hizmetlerinde, hizmet unsuru esas iken bu hizmetin sağlanabilmesi için gerekli olan bir sertifika üretilmekte ve bu sertifika ESHS'nin kendi sertifikasıyla imzalanmaktadır. Bu işlem ESHS tarafında maliyet doğurucu bir işlem olup, yaratılan sertifikanın, adına yaratıldığı kişi dışında başka bir kişi tarafından kullanılması mümkün değildir. Bu özelliğinden dolayı nitelikli elektronik sertifikalar, madde metninde belirtilen iade edilemeyecek ürünler kapsamı altında değerlendirilmelidir.

Güvenli elektronik imza oluşturma araçları ise nitelikleri itibari ile bir mal olmalarından ve madde metninde belirtilen istisnalar kapsamında bulunmadıklarından dolayı cayma hakkına konu olabileceklerdir. Ancak, güvenli elektronik imza oluşturma

aracında cayma hakkının kullanılmasıyla ilgili çeşitli sorunlar ortaya çıkabilecektir. Tüketici cayma hakkını kullanarak, aracı iade ettiğinde, kendisine ait nitelikli elektronik sertifikayla bağlı imza oluşturma verisinin de araçla birlikte geri verilmesi durumu ortaya çıkacaktır. Ancak, tüketici elektronik imza mevzuatı doğrultusunda böyle bir durumda sertifikasını iptal ettirmeli ve aracın iadesinden önce güvenli elektronik imza oluşturma verisini silmelidir. Tüketicinin nitelikli elektronik sertifikasını iade etmek istemediği fakat güvenli elektronik imza oluşturma aracını iade etmek istediği durumlarda ne olacağı tartışılması gereken bir hususdur. Burada nitelikli elektronik sertifika hizmeti sağlamanın, tüketicinin güvenli elektronik imza oluşturma aracı sahibi olmasına bağlı olduğu eğer tüketicinin aracı yoksa bu hizmetin sağlanamayacağı noktası göz önünde bulundurulmalıdır. Tüketici güvenli elektronik imza oluşturma aracını iade ettiğinde diğer hizmetin sağlanması için gerekli olan bir aracı elinden çıkardığı için ESHS kusuru bulunmadan söz konusu hizmeti yani sözleşme ile yüklendiği edimi yerine getiremeyecek ve bu durumdan sorumlu olamayacaktır. Tüketicinin güvenli elektronik imza oluşturma aracını değiştirmek istemesi söz konusu olursa bile, hizmetin sağlanması baştan belirlenen ve tüketiciyi tanımlayan araca bağlı olduğu için ESHS yine kusuru ve sorumluluğu bulunmadan hizmeti sağlamaktan imtina edebilecektir. Ancak eğer güvenli elektronik imza oluşturma aracı ayıplı mal kapsamına giriyorsa, ESHS hem güvenli elektronik imzayı hem de nitelikli elektronik sertifikayı bila bedel değiştirmek zorundadır. Söz edilen son durum sadece mesafeli sözleşmeler için değil tüm iş modellerinde geçerli olacaktır.

Yukarıda anlatılan sözleşmenin akdedilmesinden önce bildirilmesi gereken bilgiler, bu bilgilere ilişkin tüketici onayı, sözleşmede bulunması gerekli hususlar ve cayma hakkı konuları, başvurunun ve sözleşmenin internet üzerinden yapıldığı ve/veya noter aracılığıyla yapıldığı durumlarda geçerlidir. Ancak daha önce belirttiğimiz gibi tüketicinin ESHS'nin yerine gelerek bizzat başvuru yaptığı, sözleşme imzaladığı ve nitelikli elektronik sertifikasını ve güvenli elektronik imza oluşturma aracını teslim aldığı koşullarda geçerli değildir. Başvurunun internet üzerinden veya telefonla yapıldığı ve sözleşmenin teslim sırasında akdedildiği durumlar ise, Tüketicinin Korunması Hakkında Kanun kapsamında "kapıdan satışlar" olarak değil "mesafeli

sözleşme" olarak değerlendirilmelidir. Zira tüketici nitelikli elektronik sertifika alma iradesini, internet veya telefon üzerinden sipariş verdiği sırada ortaya koymaktadır.

Tüketicinin Korunması Hakkında Kanunun 6. maddesine göre; Kanunun 9/A maddesinde yazılı olarak düzenlenmesi öngörülen tüketici sözleşmeleri en az oniki punto ve koyu siyah harflerle düzenlenir ve sözleşmede bulunması gereken şartlardan bir veya birkaçının bulunmaması durumunda eksiklik sözleşmenin geçerliliğini etkilemez. Buna göre, nitelikli elektronik sertifika sözleşmeleri en az en az oniki punto ve koyu siyah harflerle düzenlenmenledir.

Yukarıda detaylı bir şekilde açıklandığı üzere nitelikli elektronik sertifika satışlarının, Tüketicinin Korunması Hakkında Kanuna tabi olacağı ve bu Kanun ve ilgili ikincil mevzuatla belirlenen hükümlerin elektronik imza uygulamasında geçerlilik bulacağı görülmektedir. Bu doğrultuda, nitelikli elektronik sertifika satışlarının sadece tüketici tarafından yapılacak tek taraflı bir taahhüt ile yapılması mümkün değildir. Telekomünikasyon Kurumu tarafından 04.02.2006 Tarih'li Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik'le ortaya konulan düzenleme ile taahhütlerin belirlenmesinin amacı, ESHS'lerin noter üzerinden başvuru almalarını kolaylaştırmak içindir. ESHS'lerin söz konusu iş modelinde tüketici, noter önünde kimlik kanıtlama işlemlerini gerçekleştirerek, elektronik imza sözleşmesinin kendi kısmını imzalamakta ve bu imzalı nüshayı ESHS'ye göndermektedir. Ancak uygulamada noterler, noter önünde imzalama işlemini sadece tarafların hepsi noter önünde hazır bulundukları takdirde gerçekleştirmektedirler. Söz konusu iş modelinin yürüyebilmesi için, noterler tarafından kabul edilebilecek tek taraflı taahhütlerin imzalanması gündeme getirilmiş ve düzenleme bu doğrultuda değiştirilmiştir. Ancak düzenleme ile ESHS'lerin iş modeli kurtarılmak istenirken mevcut diğer mevzuat sebebiyle hukuka uygun olmayan bir durum yaratılmıştır. Oysa noter aracılığıyla başvuru yöntemi, noterden alınacak imza beyannamesi aracılığı ile yapılsa, hem gerekli kimlik doğrulaması işlevi gerçekleştirilebilecek hem de tüketici sözleşmeyi kendi başına imza ederek ESHS'ye yollayabilecektir.

I. Bireysel Sözleşmeler

Bireysel sözleşmeler, ESHS ile sertifika talep eden kişi arasında yapılan sözleşmelerdir. Bireysel sözleşmelerde taraflar sözleşme serbestisi içerisinde hareket etmekle beraber Elektronik İmza Kanunu ve ilgili ikincil düzenlemelerin emredici hükümleri ile bağlıdırlar. Uygulamada bireysel sözleşmeler, bireysel başvurular için bireysel sözleşmeler ve kurumsal başvurular için bireysel sözleşmeler olmak üzere iki şekilde düzenlenmektedir. Bireysel başvurular için bireysel sözleşmeler, sertifika talep eden kişinin doğrudan kendisinin sertifika başvurusunda bulunduğu zamanda; kurumsal başvuru için bireysel sözleşmeler ise kurumsal başvuru sahibinin sertifika başvurusunda bulunduğu zamanlarda düzenlenmektedir. Uygulamada kurumsal başvuru için bireysel sözleşmeler, kurumsal başvuru sözleşmesini imzalayan kurumsal başvuru sahibinin yetkilisi tarafından, sertifika temin edilecek kişilere imzalattırılıp diğer belgelerle birlikte ESHS'ye iletilmektedir.

Bireysel sözleşmelerde genel olarak nitelikli elektronik sertifika başvurusu, sertifika sahibinin yükümlülükleri, ESHS'nin yükümlülükleri, sorumluluğun sınırlandırılması, sertifika sahibi dışında iptal, askı ve yenileme talebinde bulunabilecek kimseler, uyuşmazlık prosedürleri ve geri ödeme politikası ile ilgili hükümler bulunmaktadır[32]. Sözleşmede bulunan sorumluluğun sınırlandırılması ile ilgili hükümler, sertifikanın maddi ve kullanım kapsamına ilişkin sınırları ile bütünleştirilmelidir. Zira Elektronik İmza Kanunu'nun 13. maddesinin dördüncü fıkrasına göre, *"Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir."*

[32] Menzel T., Schweighofer E., Liability of Certification Authorities: The present legal situation and the need for abstract liability of certification authorities, User Identification & Privacy Protection, Joint IFIP WG 8.5, WG 9.6, Working Conference 1999, Schweden K., DSV, S. 161-172

Uygulamada nitelikli elektronik sertifika başvuruları çeşitli yollardan yapılabilmektedir. Bireysel kullanıcı sözleşmelerinde, sertifika talep eden kişinin seçtiği başvuru yoluna göre sözleşme ile üzerine aldığı yükümlülükler farklılık yaratabilmektedir. Uygulama da kullanılan başvuru yöntemlerinden, noter aracılığı ile başvuruda, sertifika talebinde bulunan kişi, notere giderek kimlik doğrulaması prosedürlerini işletmekte ve noter huzurunda bireysel sözleşmesini imzalamaktadır. Anacak yukarıda detaylı bir şekilde açıkladığımız üzere, noterlerin tek tarafın hazır bulunduğu sözleşmelerin kendi huzurlarında imzalanmasına karşı çıkmalarından dolayı bu yöntem uygulanamamaktadır. Yine yukarıda bahsedildiği gibi bu sorun Telekomünikasyon Kurumu tarafından sertifika başvurularının tek taraflı taahhütle alınabilmesine izin veren yönetmelik değişikliği ile ortadan kaldırılmaya çalışılmıştır. Noter aracılığı ile başvuru yönteminde, sertifika talep eden kişi ayrıca kimlik bilgilerine ait belgeleri, imzaladığı sözleşme ile birlikte ESHS'ye yollamak zorundadır. Aynı yükümlülük internet üzerinden yapılan başvurularda da geçerlidir. Ancak internet üzerinden yapılan başvurularda ortaya konan bazı modellerde sertifika talep eden kişi, sadece sertifika ön başvurusu yapmakta, kendisine ait tüm kimlik doğrulama ve ilgili resmi belgeleri toplama işlemleri, güvenli elektronik imza oluşturma aracının ve nitelikli elektronik sertifikasının teslimi sırasında yapılmaktadır.

II. Kurumsal Başvuru Sözleşmeleri

Kurumsal Başvuru, Elektronik İmza Kanunu'nda yer alamamasına rağmen, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikle tanımlanmıştır. Yönetmeliğe göre kurumsal başvuru *"bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusu"* dur. Kurumsal başvurunun Yönetmelikle düzenlenmesinin temel amacı, nitelikli elektronik sertifika kullanımını yaygınlaştırmak için başvuru prosedürlerini kolaylaştırmaktır. Bilindiği üzere nitelikli elektronik sertifika başvuruları, yüz yüze kimlik doğrulaması sonrasında kabul edilmelidir. Ancak

kurumsal başvuru bu duruma bir istisna olarak düzenlenmiştir. Yönetmeliğin 9. maddesine göre,

"ESHS, nitelikli elektronik sertifika vereceği kişilerin kimliğini; nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere göre tespit eder. Nitelikli elektronik sertifika verilecek kişi kimlik tespiti esnasında bizzat hazır bulunur.

ESHS, nitelikli elektronik sertifika verilecek kişinin kimliğinin birinci fıkra hükümlerine göre önceden tespit edilmiş olduğu hallerde veya kurumsal başvurularda kimlik tespiti için bizzat hazır bulunma şartını aramayabilir. Kurumsal başvuru sahibi, adına başvuruda bulunduğu kişilerin nitelikli elektronik sertifika taleplerini yazılı olarak belgelendirir. Nitelikli elektronik sertifika başvurusu sırasında sertifika verilecek kişiye ait kimliğin doğru ve güvenilir biçimde tespit edilmesinden ESHS sorumludur."

Görüldüğü üzere kurumsal başvurularda, kimlik tespiti için bizzat hazır bulunma şartı uygulanmamaktadır. Ancak burada madde metninden dolayı, bizzat hazır bulunmamanın hallerde kabul edilebileceğine dair belirsizlikler bulunmaktadır. Şöyle ki, madde metnine bakıldığında, bizzat hazır bulunmama için, kimlik tespitinin maddenin birinci fıkrasında belirtildiği şekilde önceden yapılması veya kurumsal başvuruda bulunulması yeterli görülmüştür. Ancak düzenlemenin esas amacı nitelikli elektronik sertifika başvuru prosedürlerinin kolaylaştırılmasıdır. Yoksa kurumsal başvuru için daha az güvenli bir yöntemin kabul edilebilir olmasını ortaya koymak değildir. Bu doğrultuda sadece kurumsal başvurularda veya sadece daha önce benzer bir şekilde kimlik tespitinin yapıldığı durumlarda bizzat hazır bulunma şartını aramamak mevcut yapının güvenliğini azaltacak ve sahte sertifika veya başkasının adına sertifika alma ihtimallerini büyütecektir. Bu sebeplerden ötürü madde yorumlanırken her iki koşul birlikte düşünülmeli ve madde metnindeki veya bağlacı yerine ve bağlacı varmış gibi yorumlanmalıdır. Yani, bizzat hazır bulunmama olanağı hem daha önce maddenin birinci fıkrasında belirtilen şekilde kimlik doğrulamasının yapılmış olması hem de kurumsal başvuruda bulunulması durumunda ortaya çıkmalıdır.

Madde metininde dikkat edilmesi gereken bir başka nokta ise, kurumsal başvuru sırasında adına sertifika talebinde bulunulan kimselerin kimlik bilgileriyle ilgili her herhangi bir yanlışlık olması halinde, bu durumdan ESHS'nin sorumlu olacağıdır. Yani kurumsal başvuru sahibinin yetkilisinin hata veya kast ile yanlış kimlik bilgilerini toplaması ve buna üzerine bu yanlış bilgilerle sertifika yayınlanması halinde, bu sertifikanın kullanımından dolayı üçüncü kişilerin uğradıkları zararlardan dolayı ESHS sorumlu olacaktır. Bu sorumluluk düzenlemeden kaynaklanan bir sorumluluk olup, kurumsal başvuru sözleşmesi ile kurumsal başvuru sahibine veya yetkilisine rücu edilebilir; ancak bu durum zarara uğrayan üçüncü kişilerin doğrudan ESHS'ye müracaat etmesini engellemez.

Söz konusu düzenleme yapılırken göz önünde bulundurulan ETSI TS 101 456 standardının 7.3.1. maddesinde belirtilen dolaylı kayıtla (indirect registration) ilgili tanımlara dikkat edilmelidir[33]. ETSI TS 101 456'nın sertifika başvurusu ile ilgili 7.3.1. maddesinin c bendinde ESHS'lerin sertifika başvurusu anında, sertifika talebinde bulunan kişinin kimliğini mevcut yasalar doğrultusunda kontrol etmesi gerektiğini belirtir. Standarda göre, kimlik kontrolü yüz yüze yapılabileceği gibi yüz yüze kontrolle benzer güvenliği sağlayan dolaylı yöntemlerle de yapılabilir, kimlik kontrolüne ilişkin olarak alınacak belgeler de kağıt ortamında alınabileceği gibi elektronik ortamda da alınabilir. Standartta dolaylı başvurur yönteminden bahsedilirken kurumsal başvurudan bahsedilmemiştir. Ancak Telekomünikasyon Kurumu doğru bir şekilde dolaylı başvurunun çerçevesini belirlerken ESHS'lerin potansiyel iş modellerini göz önüne alarak kurumsal başvuruyu düzenlemiştir. Uygulamada dolaylı başvuru daha çok bankaların ve benzeri finans kurumlarının müşterileri için talep ettiği sertifikalar için kullanılmaktadır.

Uygulamada kurumsal başvurular hem dolaylı hem de doğrudan kimlik tespiti yöntemiyle yapılabilmektedir. Dolaylı başvurularda, kurumsal başvuru sahibinin yetkilisi, adına sertifika başvurusunda bulunulan kişilerin kimlik kontrollerini

[33] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s.23

gerçekleştirmekte ve/veya kimlik kontrolüne ilişkin belgeleri toplayarak ESHS'ye iletmektedir. Doğrudan kimlik kontrolü yönteminde ise, dolaylı başvurudaki prosedür aynen yürütülmekle birlikte, ESHS yetkilisi, güvenli elektronik imza oluşturma aracını ve nitelikli elektronik sertifikayı, adına sertifika talep edilen kişiye teslim ederken kimlik kontrolünü gerçekleştirmektedir. Böylece doğrudan kimlik kontrolünün şartı olan yüz yüze kimlik kontrolü gerçekleştirilmiş olmaktadır.

III. Elektronik Sertifika Hizmetlerine İlişkin Sözleşmeler (Dış Kaynak Sözleşmeleri)

Elektronik imza mevzuatı ve ilgili uluslararası standartlara uyumun sağlanabilmesi için ESHS'ler tarafından gerçekleştirilmesi zorunlu ve ihtiyari olan çeşitli hizmetler bulunmaktadır. ESHS'ler bu hizmetleri bizzat kendi imkanları ile gerçekleştirebilecekleri gibi dış kaynak yöntemini de kullanabilirler. Dış kaynak yönteminin kullanılması halinde dış kaynak olarak hizmet veren kişi veya kurumun ilgili hizmeti yerine getirirken, hizmetle ilgili ESHS'ye ait olan yükümlülükleri yerine getirmesi gerekir. ESHS dış kaynak hizmet sağlayıcının hizmetlerini mevzuatla belirlenen çerçevede yerine getirmesinden sorumludur. Ayrıca dış kaynak sözleşmeleri, Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin ekine göre bildirim sırasında Telekomünikasyon Kurumu'na verilmelidir. Uygulamada CWA 14167-1 ile tanımlanan ESHS'ye ait "core services" hizmetlerini[34] dış kaynak olan yerine getiren firmaların çalışanları da ESHS organizasyon şeması içerisine dahil edilmekte ve bunlardan da ESHS personelinden talep edilen eğitim belgeleri, sosyal güvenlik kuruluşundan alınmış belgeler ve adli sicil kayıtları talep edilmektedir.

[34] CEN Workshop Agreement, CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, June 2003 s.15

IV. ESHS'ler Arasında Yapılan Sözleşmeler

Elektronik imza uygulamasında ESHS'ler arasında farklı niteliklerde sözleşmeler yapılabilmektedir. Bu sözleşmeler, çapraz sertifikasyon (cross-certification), çapraz tanıma (cross-recognition), köprü sertifikasyon (bridge certification) ve Elektronik İmza Kanunu'nda da belirtilen yurtdışındaki ESHS'ler ile yapılan yabancı sertifikaların geçerliliğine ilişkin sözleşmelerdir.

Çapraz sertifikasyon ve çapraz tanıma teknik olarak her iki ESHS'nin sertifika zincirinin birbirini tanıması anlamına gelmektedir[35]. Köprü sertifikasyon ise bir kök sertifikanın başka bir kök sertifika tarafından imzalanması ve bu kök sertifikanın altındaki sertifikasyon zincirindeki diğer kök sertifikaların güvenilir hale gelmesidir[36]. Bu şekilde, çapraz tanıma, çapraz sertifikasyon veya köprü sertifikasyon işlemini yapan ESHS'lerin sertifika zinciri altında bulunan bir kullanıcı (ESHS'nin kök ve varsa alt kök sertifikasına sahip olan kullanıcı), diğer ESHS'nin veya köprü sertifika otoritesinin sertifika zinciri altında bulunan bir sertifika ile imzalanmış bir veri aldığında, tanımadığı ESHS'nin kök sertifikasının güvenli olup olmadığını otomatik olarak anlayacak ve doğrulama işlemini yapabilecektir[37]. Çapraz sertifikasyon veya çapraz tanıma işlemlerinde, işlemi gerçekleştiren ESHS'ler karşı ESHS'nin güvenilir bir üçüncü taraf olduğunu karşılıklı olarak beyan ederler.

Elektronik İmza Kanunu'nun 14. maddesinde yabancı elektronik sertifikaların tanınması ve geçerliliği ile hükümler bulunmaktadır;

"Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir.

---

[35] Dumortier J., Kelm S., Nilsson H., Skouma G., Eecke P.V., The Legal and Market Aspects of Electronic Signatures, Interdisciplinary Centre For Law and Information Techonology, 1999 s. 125

[36] Polk W.T., Hastings N.E., Bridge Certification Authorities: Connecting B2B Public Key Infrastructures, National Institute of Standards and Technology, s.8

[37] Lloyd S., Fillingham D., CA-CA Interoperability, PKI Forum, March 2001, s. 3

Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılır. Bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki elektronik sertifika hizmet sağlayıcısı da sorumludur."

Maddenin ilk fıkrasında yabancı elektronik sertifikaların geçerliliğinin sağlanması için milletlerarası bir anlaşmanın yapılması öngörülmektedir. Bilindiği üzere dünya üzerinde böyle bir anlaşma daha kaleme alınmamıştır. Böyle bir anlaşmanın yapılması halinde ise kanaatimizce Telekomünikasyon Kurumu tarafından sertifikaları hukuken geçerli sayılacak ESHS'ler ve bunların kök sertifikaları yayınlanacaktır.

Maddenin ikinci fıkrasında ise, yabancı bir ESHS tarafından verilen sertifikaların yerleşil bir ESHS tarafından kabul edilmesi durumunda bu sertifikaların da nitelikli elektronik sertifika olarak sayılacağı belirtilmiştir. Yurtdışında konuyla ilgili yapılan düzenlemelerin aksine, yabancı sertifikaların ülkemizde nitelikli olarak kabul edilmesi için yayınlandıkları ülkede akredite edilmiş olmaları veya nitelikli elektronik sertifika statüsünde olmaları gerekmemektedir. Kanaatimizce yabancı sertifikaların tanınması işlemi, yabancı ESHS ve yerleşik ESHS arasında yapılacak bir çapraz sertifikasyon veya çapraz tanıma işlemiyle gerçekleşecektir. Madde metninde ayrıca anlaşma sonucu tanınan sertifikaların kullanılması sonucunda doğacak zararlardan dolayı, tanıma işlemini gerçekleştiren ESHS'nin sorumlu olacağı belirtilmiştir. Yabancı sertifikaların tanınmasına ilişkin sorumluluğun düzenlenmesi konusu ne yazık ki kötü bir şekilde ifade edilmiş ve madde metninden ESHS'nin yabancı sertifikanın kullanımından doğan tüm zararları tazmin yükümlülüğü varmış gibi bir durum ortaya çıkarılmıştır. Oysa yabancı sertifikaları tanıyan ESHS'nin sorumluluğu da kendi nitelikli elektronik sertifikalarına karşı olan sorumluluk rejimiyle aynı olmalıdır. Zira ESHS'nin hiçbir kusuru olmadığı halde sertifikanın kullanımından dolayı zarar doğabilir.

V. Güvenen Taraf Sözleşmesi

Güvenen taraf sözleşmesi (relying party agreement), imzalı belgeyi alan üçüncü kişinin, doğrulama işlemini yapmadan önce kabul etmesi gereken sözleşmedir. Ülkemizdeki uygulamada bu sözleşme hukuki statüsünün belirsizliğinden ve üçüncü tarafların yükümlülüklerinin Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikle belirlenmesinden dolayı kullanılmamaktadır.

Güvenen taraf sözleşmelerinde, üçüncü kişilerin imzalı belgeyi kabul etmeden önce ESHS tarafından belirlenmiş olan kuralları kabul etmesi gerekliliği, üçüncü kişilerin doğrulamaya ilişkin yükümlülükleri, ESHS'ye ait sorumluluğun sınırlandırılması gibi konularda hükümler bulunmaktadır. Güvenen taraf sözleşmesinde genellikle doğrulama işlemini yapacak olan üçüncü kişinin güvenen taraf sözleşmesini onaylamadığı takdirde imzaya ve sertifikaya güvenerek işlem yapmaması gerektiği aksi takdirde ESHS'nin hiçbir sorumluluk kabul etmeyeceği belirtilir.

B. SERTİFİKA İLKELERİ, SERTİFİKA UYGULAMA ESASLARI

Elektronik imza uygulamasında kullanılan dokümanlar arasında belki de en önemlileri sertifika uygulama esasları (certificate practice statements) ve sertifika ilkeleridir (certificate policy) . Sertifika uygulama esasları ve sertifika ilkeleri, belirli sertifika uygulamasının temel çerçevesini belirleyen, uygulamayla ilgili tüm şart ve koşulları ortaya koyan belgelerdir[38]. Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelikte, sertifika ilkeleri "*ESHS'nin işleyişi ile ilgili genel kuralları içeren belge*", sertifika uygulama esasları ise "*Sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belge*" olarak

[38] European Commission in the framework of the SPRITE-S² pilot action, Guidelines, Methodologies and Standards to set up a CA for Digital Signatures, s. 28

tanımlanmıştır. Bu tanım, sertifika ilkelerinin ve sertifika uygulama esaslarının açık anahtarlı altyapı uygulamaları içerisindeki rolü ve kullanımı dikkate alındığında ne yazık ki oldukça yetersiz ve eksik kalmaktadır.

I. Sertifika İlkeleri

Sertifika ilkeleri dokümanıyla ilgili ilk tanım X.509 çalışma grubu tarafından yapılmıştır. X.509 sertifika ilkelerini "sertifikanın uygulanabilirliğini belirli bir topluluğa ve/veya yaygın güvenlik gereksinimleri ile bir uygulama sınıfına ifade eden, isimlendirilmiş kurallar bütünü"[39] olarak tanımlar.

Burada dikkat edilmesi gereken en önemli husus, sertifika ilkelerinin, Yönetmelikte belirtilenin aksine sadece ESHS tarafından yayınlanmak veya onaylanmak zorunda olmayışıdır. Sertifikaya güvenerek işlem yapacak bir üçüncü taraf, sertifikayı kullanarak imza atacak imzalayan, imza uygulamasını geliştiren ve kullanıma sunan taraf bir sertifika ilkesi yayınlayıcısı olabilir[40]. Zira ESHS'lerin sertifikaları kullanılarak, ESHS'nin ilkeleriyle uyumlu fakat, ESHS'nin ilkelerine göre daha detaylı kriterlerin belirlendiği sertifika uygulama alanları olabilecektir. Örnek vermek gerekirse, Baro aracılığıyla başlatılacak bir elektronik imza uygulamasında, sertifika başvuru prosedürleri, avukatların kullanacağı elektronik imza uygulamaları, avukatların uymaları gereken güvenlik gereksinimleri farklılık arz edebilir. Böyle bir durumda Baro ESHS'nin sertifika ilkeleriyle uyumlu bir ilke yayınlayarak kendi uygulaması için spesifik şartlar ve koşullar belirleyebilir. Ancak burada dikkat edilmesi gereken, Baronun uygulamasında çalışacak sertifikaları yayınlayan tüm ESHS'lerin ilkeleriyle uyumlu bir ilke yayınlanmasının zorunluluğudur. Eğer Baro belirlediği ilkelerde, tüm ESHS'lerin yayınladığı sertifikaların uygulamada geçerli olacağını belirtiyorsa bu

[39] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," 1997

[40] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s. 9

durumda tüm ESHS'leri sertifika ilkeleriyle uyumlu bir ilke yayınlamalıdır. Ancak Baro sadece belirli ESHS'lerin sertifikaların kabul edileceği bir uygulama geliştiriyorsa bu durumda kabul edilen sertifikaları kendi sertifika ilkeleri dokümanında belirtmelidir; bu durumda Baro sadece kabul ettiği sertifikaları yayınlayan ESHS'nin ilkeleriyle uyumlu bir ilke yayınlayabilir.

X.509 tarafından yapılan tanımda da belirtildiği gibi sertifika ilkeleri iki sınıfa ayrılabilir. Bunlardan biri "sertifikanın uygulanabilirliğini belirli bir topluluğa" ifade eden sertifika ilkeleri, diğeri ise "sertifikanın uygulanabilirliğini yaygın güvenlik gereksinimleri ile bir uygulama sınıfına" ifade eden sertifika ilkeleridir[41]. Sertifikanın uygulanabilirliğini belirli bir topluluğa ifade eden sertifika ilkeleri, sertifikanın kullanılabileceği alanları ve uygulamaları yine kendi içerisinde belirlediği topluluğa uygular. Bu topluluk, yukarıda verilen örnekte olduğu gibi Baro üyeleri, herhangi bir bankasının internet kullanıcıları, bir kamu kurumunun çalışanları olabilir. Sertifika ilkeleri, topluluğu coğrafi sınırlar ile de belirleyebilir. ETSI TS 101 456 ile belirlenen topluluk, Elektronik İmza Direktifi ile uyumlu nitelikli elektronik sertifikaların kullanıldığı ülkelerdir. Ülkemizde ESHS'ler tarafından kullanılan sertifika ilkelerinin, uygulandığı topluluk Türkiye sınırları içerisinde ESHS'nin yayınladığı nitelikli elektronik sertifikalarla işlem yapan veya işlemle bağlantılı olan kimselerdir. Daha önce belirttiğimiz gibi ESHS'nin yayınladığı sertifika ilkelerinin altında ayrı bir sertifika ilkesi yayınlayan kişi veya kurum ESHS'nin yayınladığı sertifika ilkeleriyle belirlenen topluluğu sınırlandırabilir, ancak genişletemez.

Sertifikanın uygulanabilirliğini yaygın güvenlik gereksinimleri ile bir uygulama sınıfına ifade eden sertifika ilkeleri ise aynı uygulama alanı içerisinde birden fazla sertifika sınıfı yaratılmasını sağlar. Sertifika sınıfları, gerektirdikleri güvenlik yapısı, kullanım alanları, kullanım sınırları veya sigorta sınırları gibi farklı niteliklerle ayrıştırılabilir. Örnek vermek gerekirse Verisign Inc. tarafından yaratılan sertifikalar, üç

[41] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s.10

ayrı sınıfa ayrılmaktadır[42]. Class 1, Class 2 ve Class 3 sertifikaları güvenlik yapısı bakımından hiçbir farklılık arz etmemelerine rağmen, kullanım alanları, sigorta güvenceleri ve sertifika başvuru prosedürleri açısından farklılık göstermektedirler. İlk ki sınıfın başvurusu internet üzerinden yapılabilirken, üçüncü sınıf yüz yüze başvuruyu gerektirmektedir. İlk iki sınıf sertifikanın dahil olduğu sigorta kapsamı da aynı şekilde üçüncü sınıfa göre daha düşüktür.

ETSI TS 101 456 da, sertifika sınıfı olarak iki sınıf belirlemiştir. Bunlardan birisi sadece nitelikli elektronik sertifikalara uygulanan QCP public, diğeri ise güvenli elektronik imza oluşturma aracı ile birlikte kullanılan nitelikli elektronik sertifikalara uygulanan QCP public + SSCD ilkeleridir[43]. ETSI TS 101 456 sertifika ilkelerine göre, her iki sınıf için belirlenen katılımcılara ait yükümlülükler ve gereksinimler değişmektedir. Ülkemizdeki uygulamada bir ESHS söz konusu sınıf ayrımına giderek sertifikalarını A, B ve C sertifikaları olarak üçe ayırmıştır[44]. Bu sertifikalar kullanım alanları, kullanım sınırları, sertifikanın içerdiği bilgiler ve başvuru prosedürleri olarak birbirinden ayrılmaktadır. Belirtmek gerekir ki sertifika ilkelerinin topluluk veya sınıf olarak ayrıştırılması, her biri için ayrı doküman yaratılmasını gerektirmez. Aynı sertifika ilkeleri dokümanında farklı sınıf ve topluluk için farklı sertifika ilkeleri belirlenebilir.

Sertifika ilkeleri, kamuya açık veya gizli bir doküman olarak hazırlanabilir[45]. Burada kastedilen gizlilik, sadece ilgili açık anahtarlı altyapıdaki katılımcıların erişebilmesi olarak algılanmalıdır. Bunu dışında sertifika ilkeleri, eğer açık anahtarlı altyapı kamuya yönelik bir uygulamaysa kamuya açık olarak yayınlanmalıdır. Nitelikli elektronik sertifikalar gibi kamuya açık uygulamalarda sertifika ilkelerinin kamuya açık

---

[42] VeriSign,Inc., VeriSign Trust Network Certificate Policies, Version 2.0, December 2004

[43] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s. 14

[44] http://www.e-guven.com/default.asp?ID=7&site=2

[45] Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, PKI Assesment Guidelines, American Bar Association publishing, June 2001 s. 314

olması hatta herkes tarafından erişilebilir olması ESHS'nin yükümlülüğüdür. Ancak kamuya açık sertifika ilkelerinin dahi belirli bölümleri bilgi güvenliğinin sağlanması açısından gizli tutulabilir. Bu bölümler özellikle fiziki alan ve anahtar kontrollerine ilişkin bilgilerdir.

Bir elektronik sertifikaya ait sertifika ilkesini, üçüncü tarafların görebilmesi ve bu doğrultuda sertifika ilkelerinin hükümleri altında işlem yapabilmesi için sertifikanın içerisinde sertifika ilkelerine ait tanımlayıcılar bulunmaktadır. Bu tanımlayıcılar eşsiz numaralar olarak sertifikanın içerisinde önceden belirlenmiş alanlara girilirler[46]. Bu tanımlayıcılara nesne belirteci (OID, object identifier) denilmektedir. Nesne belirteçleri ağaç yapısı ile kullanılmakta, her dal kendi kapsamı altındaki alt dallara ayrılmaktadır. Nesne belirteçleri ISO/IEC ve ITU standartları doğrultusunda OID kayıt birimleri tarafından verilmekte ve her kayıt için ayrı bir numara verildiği için numaraların eşsizliği sağlanmaktadır. Bir OID numarasını alan ilgili, bu numaranın altında alt dallar açarak kendi uygulamalarını ve dokümanlarını eşsiz numaralar ile tanımlayabilir.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 7. maddesine göre nitelikli elektronik sertifikalar, ETSI TS 101 862 ve ITU-TRec. X.509V.3'e uygun olarak oluşturulmalıdır. ITU-TRec. X.509 V.3 elektronik sertifikanı teknik yapısını ve içeriğini belirlerken; ETSI TS 101 862 ise 99/93/EC sayılı Elektronik İmza Direktifi kapsamındaki nitelikli elektronik sertifikaların içeriğine ilişkin gereksinimleri ortaya koymaktadır.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 7. maddesine göre ESHS; sertifika ilkelerini ve sertifika uygulama esaslarını IETF RFC 3647'ye uygun olarak hazırlar. RFC 3647, IETF Network Çalışma Grubu tarafından hazırlanmış olan sertifika ilkeleri ve sertifika uygulama esasları çerçevesidir. Doküman, ESHS'ler, ilke yayınlayıcılar ve elektronik sertifikalara güvenerek işlem yapacak üçüncü kişiler gibi sertifika ilkesi ve sertifika uygulama esasları hazırlayanlar için bir

[46] Network Working Group, Internet X.509 RFC 3280 Certificate and Certificate Revocetion List Profile, April 2002 s.30

başvuru dokümanı olarak yaratılmış aynı zamanda karşılıklı işlerlik ve standardizasyon sağlanabilmesi amaçlanmıştır. RFC 3647, içerik olarak zorunluluk unsurları taşımamakta daha çok sertifika ilkeleri ve sertifika uygulama esasları için taslak çerçeveyi çizmektedir. Uygulamada Telekomünikasyon Kurumu da ESHS'lerden RFC 3647 çerçevesini ve başlıklarına tam uyum sağlanmasını ve RFC 3647'de belirtilen tüm başlıkların ESHS'lerin sertifika ilkeleri ve sertifika uygulama esasları dokümanlarında bulunmasını istemektedir.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 9. maddesine göre ESHS; güvenlik kriterlerine ilişkin olarak; CWA 14167-1, ETSI TS 101 456 ve TS ISO/IEC 17799 veya ISO/IEC 17799 standartlarına uyar. Tebliğin 5. maddesine göre ise ESHS işleyişinin bütün aşamalarında ETSI TS 101 456 ve CWA 14167-1 standartlarına uyar. Burada bahsedilen ETSI TS 101 456 standardı aslında 99/93/EC sayılı Elektronik İmza Direktifi kapsamında nitelikli elektronik sertifikaları yayınlayan ESHS'lerin sertifika ilkelerine ilişkin gereksinimlerinin ortaya konduğu bir dokümandır. Bu sebepten ötürürü Tebliğ'deki her iki maddede belirtilen gereksinimler ESHS'nin sertifika ilkeleri ve sertifika uygulama esasları dokümanlarıyla da ortaya konulmalıdır.

II. Sertifika Uygulama Esasları

Sertifika uygulama esasları, Amerikan Barolar Birliği Bilgi Güvenliği Komitesi tarafından, "sertifika otoritesinin sertifika yayınlarken kullandığı uygulamalara ilişkin beyan" olarak tanımlanmıştır[47]. Sertifika uygulama esasları, sertifika otoritesinin hizmetlerini sunarken, teknik, iş ve hukuksal olarak ortaya koyduğu niteliklerini ve prosedürlerini açıkladığı belgedir[48].

[47] Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, PKI Assesment Guidelines, American Bar Association publishing, June 2001, s. 29

[48] Ferrer-Gomila J., Payeras-Capellà M., Certification Practise Statements: The National Mint of Spain's Experience, UPGRADE Vol. V, No. 3, June 2004 s. 16

Burada dikkat edilmesi gereken en önemli husus, sertifika ilkelerinden farklı olarak, sertifika uygulama esaslarının sadece sertifika otoriteleri tarafından yayınlanıyor olmasıdır. Çünkü sertifika uygulama esasları, sertifikaya ilişkin koşullardan çok sertifika otoritesine ilişkin nitelikleri ortaya koymaktadır.

Sertifika uygulama esasları, sertifika otoritesi tarafından detaylı bir şekilde belirlenmek istenmeyebilir. Uygulamanın özelliğine göre kullanıcılarla yapılan, sertifika sahibi sözleşmesi veya güvenen taraf sözleşmesi, sertifika uygulama esasları yerine geçebilir[49]. Sertifika uygulama esasları, sertifika otoritesinin işleyişine ve özelliklerine ilişkin detaylı bilgi verdiği için bir bilgi güvenliği riski yaratabilir. Bu sebeple, sertifika otoritesi sertifika uygulama esaslarının bir bölümünü yayınlayamayabilir veya içeriğe ilişkin özet bilgi verebilir. Sertifika uygulama esaslarının kamuya açık olması ise kullanıcılara kullanılan sistemin ne kadar güvenli olduğunu göstermek ve garanti etmek için en önemli yoldur. Ülkemizde mevzuat ile belirlenen zorunluluklardan dolayı bütün ESHS'ler sertifika uygulama esaslarını yayınlamak zorundadırlar.

III. Sertifika İlkeleri ve Sertifika Uygulama Esaslarının Karşılaştırılması

Genel olarak belirtildiği üzere, sertifika otoritesi operasyonlarında ve sertifika uygulamalarında, sertifika ilkeleri neyin yapıldığını belirlerken sertifika uygulama esasları nasıl yapıldığını ortaya açıklamaktadır. Sertifika ilkeleri uygulama içerisindeki gereksinimleri belirlerken, sertifika uygulama esasları ilkelerin belirlediği gereksinimlerin nasıl uygulandığını belirtir[50].

[49] Certification Practice Statement and Subscription Agreement ("CPS") For Wireless Application Protocol (WAP) Server Test Certificates, Version 1.0, November 2000

[50] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s.16

Sertifika ilkeleri; sertifika otoriteleri, güvenen taraflar ve uygulama sağlayıcılar/geliştiriciler tarafından yayınlanırken; sertifika uygulama esasları sadece sertifika otoriteleri tarafından yayınlanmaktadır. Bu durumda ülkemizdeki uygulamada da olduğu gibi, bir ESHS birden çok sertifika ilkeleri ile çalışabilirken tek bir sertifika uygulama esasları yayınlamaktadır.

IV. Sertifika İlkeleri ve Sertifika Uygulama Esaslarının Hukuki Statüsü

Yukarıda detaylı bir şeklide açıklandığı üzere sertifika ilkeleri ve sertifika uygulama esasları, ESHS'nin bilgi kaynaklarıdır. İlkeler ve esaslar aynı zamanda ESHS'nin değerlendirilmesi için en önemli argümanları ortaya koyarlar[51]. ESHS, sertifika ilkeleri ve sertifika uygulama esasları ile kendi işleyişine dair tüm detayları kamuoyuna ve ilgili taraflara bildirir[52]. Sertifika ilkeleri ve sertifika uygulama esasları hukuki olarak tek taraflı taahhüt niteliğindedir. Burada taahhüt eden ESHS, taahhütleri herkese karşı ortaya koymaktadır. Yani sadece sertifika kullanıcıları değil sertifika ilkeleri ve uygulama esaslarının kapsamındaki tüm katılımcılar ESHS'den ilkeler ve esaslara uymasını isteyebilirler. ESHS, mevzuatla üstlendiği yükümlülüklerin yanı sıra sertifika ilkeleri ve uygulama esasları ile bildirdiği ve üstlendiği yükümlülüklerle de sorumludur.

Sertifika uygulama esaslarının kapsamı altında kalan katılımcılar ise sertifika uygulama esaslarındaki hükümlerle doğrudan sorumluluk altına girmezler. Bu sebepten ötürü uygulamada, sertifika sahibi sözleşmelerinde ve güvenen taraf sözleşmelerinde, sertifika ilkeleri ve sertifika uygulama esasları dokümanı, sözleşmenin ayrılmaz bir parçası olarak gösterilir ve taraflar bu dokümanlarla bağlı hale getirilir.

---

[51] Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, PKI Assesment Guidelines, American Bar Association publishing, June 2001, s.29

[52] Nilsson H., Eecke P.V., Medina M., Pinkas D., Pope N., European Electronic Signature Standardization Initiative (EESSI), Final Report of the EESSI Expert Team, July 1999 s. 39

Denetleme kurumu (uygulamada bu kurum Telekomünikasyon Kurumu veya özel bir uygulamada ilgili kurum olabilir), ESHS'yi uluslararası standartlara ve mevzuata uyumunun yanı sıra kendi sertifika ilkeleri ve uygulama esaslarına uyumluluğu açısından da denetlemelidir.

V. Sertifika İlkeleri ve Sertifika Uygulama Esaslarının Genel Çerçevesi

Bu bölümde RFC 3647 standardına uygun bir sertifika ilkeleri ve/veya sertifika uygulama esaslarının ETSI TS 101 456 gereksinimleri de göz önünde bulundurularak, genel çerçevesi ve içermesi gereken temel bilgiler ele alınacaktır.

RFC 3647'ye göre sertifika ilkeleri ve/veya sertifika uygulama esaslarının temel olarak aşağıda detaylı olarak açıklanan dokuz ana başlıkta bilgi içermesi gerekmektedir.

1. Giriş (Introduction)

Bu bölümde dokümanın kapsamı ve amacı açıklanmaktadır. Elektronik İmza Kanunu kapsamında ESHS'ler bu bölümde mevzuata atıf yaparak ESHS yetkileri ile ilgili bilgileri ve sertifika ilkeleri ve uygulama esaslarının yayınlanma amacını belirtmelidirler.

1.1. Genel (Overview)

Giriş bölümünün alt başlığı olarak burada, tüm dokümana ait genel bir giriş yapılarak, sertifikasyon yapısı ve ilgili taraflarla ilgili genel bilgi verilir. ESHS bu bölümde, ESHS ve ilgili diğer kavramlarla ilgili temel tanımları yapmalı ve güvenli elektronik imza ve nitelikli elektronik sertifika hakkında temel bilgi vermelidir.

Sertifika ilkeleri dokümanında ETSI TS 101 456 da belirtilen iki sertifika sınıfından (QCP, QCP+SSCD) hangilerinin desteklendiği de belirtilmelidir[53].

1.2. Doküman Adı ve Tanımlama (Document Name and Identification)

Bu bölümde dokümanların tam adı, yayınlanma bilgileri ve varsa kendilerine ait nesne belirteçleri belirtilir[54].

1.3. Katılımcılar (PKI Participants)

Bu başlık altında dokümanın kapsamına giren taraflar belirlenir ve tanımları yapılır. Elektronik imza uygulamasında katılımcılar, ESHS, kayıt birimleri, sertifika sahibi, üçüncü kişiler ve ESHS'nin operasyonlarını gerçekleştirdiği yüksek güvenlikli güven merkezidir.

1.4. Sertifika Kullanımı (Certificate Usage)

Bu bölümde, sertifika ilkelerinde kabul edilen sertifikalar belirtir. Sertifikanın kullanım alanları ve geçerliliği açısından izin verilen ve verilemeyen durumlar ortaya konulur. ESHS'ler bu bölümde; ESHS'nin kök ve alt kök sertifikalarının sadece nitelikli elektronik sertifika imzalanması, sertifika iptal listelerinin imzalanması, çevrim içi sertifika durum protokolü (OCSP) bilgilerinin imzalanması ve zaman damgası sertifikalarının imzalanması ile bu sertifikaların ve verilerin doğrulanması süreçlerinde kullanılabileceğini belirtmelidirler[55].

---

[53] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s.16

[54] ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, V1.2.2, Valbonna – France, 2005 s. 15

[55] Certipost E-Trust Services, Certification Practice Statement for Qualified and Normalised Certificates, Version 1.0, December 2003 s.84

ESHS tarafından oluşturulan nitelikli elektronik sertifikalar sadece güvenli elektronik imza oluşturma ve doğrulama süreçleri içersinde, sertifikanın içinde yer alan kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanılmalıdırlar. Nitelikli elektronik sertifikalar aynı zamanda üçüncü kişiler tarafından sertifikanın geçerliliğinin doğrulanması ve sertifika içeriğine erişilmesi amaçlarıyla da kullanılabilirler.

Elektronik İmza Kanunu'nun 5. maddesi hükmü uyarınca "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri" güvenli elektronik imza kullanılarak yapılamaz. Bundan dolayı nitelikli elektronik sertifikalar bu işlemlerde kullanılamaz.

1.5. Politika Yönetimi (Policy Administration)

Bu bölümde sertifika ilkelerini ve/veya uygulama esaslarını geliştiren, güncelleyen, onaylayan ve yayınlayan kişi ve/veya kurumun adı, adresi ve iletişim bilgileri bulunur. Ayrıca sertifika ilkelerinin ve/veya uygulama esaslarının geliştirilme, güncellenme, onaylanma ve yayınlanma prosedürleri açıklanır.

1.6. Tanımlar ve Kısaltmalar (Definition and Acronymes)

Bu kısımda sertifika ilkeleri ve/veya uygulama esaslarında kullanılan kavramlara ilişkin tanımlar ve kısaltmaların açıklamaları bulunur.

2. Yayınlama ve Bilgi Deposu Sorumlulukları (Publication and Repository Responsabilities)

ESHS'ler mevzuat doğrultusunda yayınladıkları nitelikli elektronik sertifikaları, sertifika iptal listelerini, sertifika ilkelerini ve uygulama esaslarını, kullanıcı sözleşmelerini, bilgilendirici dokümanları ve ilgili görsel ve işitsel yayımları

bilgi deposunda yayınlar. Bilgi deposu ilgili herkesin erişimine 7/24 hizmet verecek şekilde erişime açık bulundurulur.

3. Tanımlama ve Kimlik Doğrulama (Identification and Authentication)

ESHS nitelikli elektronik sertifika başvuru sahiplerine sertifika temin etmeden önce başvuru sahibinin kimlik bilgilerini, sertifika içerisinde yer alacak bilgilerini, sertifika kullanılmasıyla ilgili yetkilerini resmi kayıtlara dayanarak doğrulamalıdır.

3.1. İsimlendirme (Naming)

Nitelikli elektronik sertifikalarda, sertifika sahibinin adı, kimlik doğrulama sırasında vermiş olduğu resmi belgelerde belirtilen adla aynı olmalıdır. ESHS'nin Kök ve Alt Kök Sertifikalarında, ESHS'nin gerekli prosedürleri tamamlamış bir ESHS olduğuna dair kayıt ve ticari unvan bulunur[56].

Elektronik İmza Kanunu'na göre nitelikli elektronik sertifikalarda takma isim kullanımı ve/veya sertifika sahibinin ismini gizlemesi mümkün değildir. Nitelikli elektronik sertifikalarda, sertifika sahiplerinin isimlerinin aynı olma ihtimali vardır; bu durumda ayrıştırılma için sertifikaların eşsiz bilgilerle tanımlanması gerekir. Bu eşsiz bilgiler T.C. vatandaşları için T.C. kimlik numarası, yabancı uyruklular için pasaport numarası ile sağlanır.

3.2. İlk Kimlik Doğrulaması (Initial Identity Validation)

ESHS tarafından doğru kişiye doğru bilgilerle nitelikli elektronik sertifika sağlanabilmesi için sertifika sahibinin, imza oluşturma verisinin zilyetliğine sahip olduğunun kanıtlanması gerekmektedir. Kanıtlanma ESHS'nin sertifika sağlama

[56] e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları, Kasım 2005 s. 12

modeline gör iki şekilde yapılabilir. ESHS, güvenli elektronik imza oluşturma aracını sağlamıyorsa veya aracı nitelikli elektronik sertifika yüklü olmadan sağlıyorsa internet üzerinden ve PKCS 11 aracılığıyla sertifika sahibinin imza oluşturma verisine sahip olduğu kanıtlanır. Ancak ESHS güvenli elektronik imza oluşturma aracını nitelikli elektronik sertifika yüklü olarak sağlıyorsa, imza oluşturma verisinin sertifika talep eden kişide bulunma ihtimali yoktur, burada kimlik kontrolü imza karşılığı araç teslimi ile kanıtlama prosedürü tamamlanır.

Tüzel kişilerin kimliklerinin doğrulanması safhası için; kurumsal başvurularda ve/veya nitelikli elektronik sertifika içerisine ilgili tüzel kişi adına yetki ile ilgili bilgi konulması gerektiği takdirde, tüzel kişinin kimliği resmi belgelere dayanılarak doğrulanır. Bireylerin kim kimliklerinin doğrulanması safhası için ise; kişinin kimliği nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli bir belgeye dayanılarak ve yüz yüze kimlik doğrulaması yoluyla tespit edilir[57].

3.3. Yeniden Anahtarlama için Tanımlama ve Kimlik Doğrulama (Identification and Authentication for Re-key Requests)

Nitelikli elektronik sertifikaların geçerlilik süresi bitmeden önce eğer sertifika kullanılmaya devam edilmek isteniyorsa geçerlilik süresi uzatılmalı ve sertifika yenilenmelidir[58]. Sertifika yenilenmeden önce kimlik doğrulaması işlemleri tekrar yapılmalıdır. Bu gereksinim, sertifika sahibinin kimliğinin yüz yüze kontrol edilmesiyle veya kendisinden alınacak güvenli elektronik imzalı bir yenileme formuyla gerçekleştirilebilir.

[57] Politique de Certificat Relative Au Certificat Qualifie Ou Normalise Certipost E-Trust, Version 1.0, Mai 2004 s. 8

[58] VeriSign Trust Network Certificate Policies, Version 1.3, March 2004 s. 49

3.4. İptal Talebi için Tanımlama ve Kimlik Doğrulama (Identification and Authentication for Revocation Requests)

İptal ve askıya alma talepleri için bu talebi yapan kişinin veya kurumun iptal ve askıya alma için yetkisinin bulunup bulunmadığının kontrolünün yapılması gereklidir. Sertifika sahibi, kurumsal başvuru sahibi, sertifika sahibinin yetkilendirdiği üçüncü kişiler, iptal ve askıya alma yetkisine sahip olabilirler. Bu yetki ESHS tarafından verilen parolalar veya kimlik bilgileri aracılığıyla kontrol edilir ve yetki doğrulaması yapıldıktan sonra iptal ve askıya alma işlemi gerçekleştirilir[59].

4. Sertifika Yaşam Zinciri Operasyonel Gereklilikler (Certificate Life-Cycle Operational Requirements)

Bu bölümde ESHS'nin temel fonksiyonları, ve hizmetlerinin yerine getirilmesiyle ilgili prosedürler yer almaktadır.

4.1. Sertifika Başvurusu (Certificate Application)

Bu bölümde bireysel ve kurumsal başvuru modelleri, başvuru prosedürleri, yüz yüze ve dolaylı kimlik doğrulama prosedürleri, başvuru için gerekli belgeler hakkında bilgi verilir.

4.2. Sertifika Başvuru Süreci (Certificate Application Processing)

Bu bölümde yapılan başvuruların ESHS ve varsa kayıt birimi tarafından değerlendirilmesi ve geri dönüş prosedürleri anlatılmaktadır.

[59] VeriSign Certification Practice Statement, Version 2.3, March 2004 s. 47

4.3. Sertifika Oluşturulması (Certificate Issuance)

Bu bölümde, sertifika talep eden kişiden alınan geçerli sertifika başvurusu üzerine, ESHS'nin sertifikanın oluşturulması için yaptığı işlemler ve sertifikanın sertifika talep eden kişiye ulaştırılması ile ilgili prosedürler anlatılmaktadır. İmza oluşturma verisinin sertifika talep eden kişi tarafından oluşturulması veya ESHS tarafından oluşturulması durumlarında farklı sertifika oluşturma ve teslim prosedürleri ortaya çıkacaktır.

4.4. Sertifikanın Kabulü (Certificate Acceptance)

Sertifikanın kabulü, sertifika sahibinin sertifikasını aldığının kanıtlanması, sertifika sahibinin aldığı sertifikayı kontrol etmesi ve bir eksiklik veya yanlışlık varsa ESHS'yi haberdar etmesi süreçlerini belirler. Sertifika sahibi, elektronik imza mevzuatı doğrultusunda sertifikada gerçeği yansıtmayan bir bilgi varsa derhal ESHS'yi haberdar etmelidir.

4.5. İmza Oluşturma ve Doğrulama Verileri, Sertifika Kullanımı (Key Pair and Certificate Usage)

Elektronik İmza Kanunu ve ilgili ikincil mevzuat doğrultusunda nitelikli elektronik sertifika sahipleri; imza oluşturma ve doğrulama verilerini sadece güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanabilirler. Sertifikalar eğer bulunuyorsa kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanılmalıdır. Sertifika sahibi imza oluşturma verisinin ve aktivasyon verisinin güvenliğini sağlamak ve izinsiz kullanımlarını engellemekle yükümlüdür. Sertifika sahibi, imza oluşturma verisinin gizliliği veya güvenliği konusunda şüphe duyması, imza oluşturma verisinin, imza oluşturma aracının veya aktivasyon verisinin kaybolması, çalınması veya güvenilirliğinden şüphe duyması halinde derhal ESHS'yi bilgilendirmelidir[60].

[60] e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları, Kasım 2005 s. 23

Güvenli elektronik imzaya güvenerek iş ve işlem yapacak olan üçüncü kişiler öncelikle güvenli elektronik imza ile bağlı ile olan nitelikli elektronik sertifikanın kontrolünü yapmalıdırlar. Bunun yanında yapılması gereken kontroller sertifikanın geçerlilik süresi içersinde güvenli elektronik imzanın oluşturulması, sertifikanın iptal edilmediğinin veya askıya alınmadığının tespitidir. Son olarak üçüncü kişiler güvenli elektronik imza kullanılarak yapılan işlemin mevzuatla yasaklanan hukuki işlemlerden biri olmadığını ve yapılan işlemin sertifika içersinde yer alan maddi kapsama veya kullanıma ilişkin sınırlamalara aykırı olmadığını tespit etmekle yükümlüdür.

4.6. Sertifika Yenileme (Certificate Renewal), 4.7. Sertifika Yeniden Anahtarlama (Certificate Rekey)

Elektronik sertifikalar geçerlilik süreleriyle sınırlıdır. Eğer kullanıcı, elektronik sertifikayı kullanmaya devam etmek istiyorsa yenilemelidir. Yenileme işlemi yeniden anahtarlama ve yenileme olarak iki farklı şekilde yapılamaktadır. Yenileme sertifikaya bağlı imza oluşturma ve doğrulama verilerinin değiştirilmeden, sertifikanın yenilenmesidir. Yeniden anahtarlama ise, sertifikanın yeniden yaratılması gibi baştan imza oluşturma ve doğrulama verilerinin yaratılmasıdır[61].

4.8. Sertifikanın Değiştirilmesi (Certificate Modification)

Sertifikanın içeriği, sertifika sahibinin, sertifikada bulunan bilgilerinin değişmesi sebebiyle güncellenmek zorunda kalabilir. Sertifikada değiklik yapılacak bilgilerin aynı ilk başvuru sırasında olduğu gibi resmi belgelere dayanarak doğrulanması gerekir.

[61] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s. 30

4.9. Sertifikanın İptali ve Askıya Alınması (Certificate Revocation and Suspension)

Bu bölüm altında, sertifikanın iptalini gerektiren durumlar, iptal başvurusunda kimlerin bulunabileceği (sadece yetkili kişiler gerekli yetki doğrulanmasından sonra), sertifika iptal prosedürleri, sertifika iptal talebi gecikme periyodu, ESHS'nin iptal talebini işleme koyma süresi, iptal durumuna ilişkin üçüncü kişilerin kontrol yükümlülüğü, sertifika iptal listesi yayınlama sıklığı, çevrimiçi iptal kontrolü, sertifikanın askıya alınması ile ilgili koşullar hakkında ESHS'nin işleyişi anlatılır[62].

4.10. Sertifika Durum Hizmetleri (Certificate Status Services)

Bu bölümde sertifikaların yayınlandığı LDAP sunucusu hakkında bilgiler, çevrimiçi sertifika durum kontrolü protokolünün ve sertifika iptal listesinin kullanılabilirliği ve bunlara ilişkin servis düzeyi hakkında bilgi verilir.

4.11. Sertifika Sahipliğinin Sona Ermesi (End of Subscription)

Sertifika sahibinin sertifika sahipliği, geçerlilik sürelerinin sonunda, iptal edilmeleri halinde veya ESHS kendi imza oluşturma verinsin tehlikeye düşmesi halinde sona erer.

4.12. İmza Oluşturma Verisi Kurtarma ve Yedekleme (Key Escrow and Recovery)

ESHS, iş sürekliliğinin sağlanması ve felaketten kurtarma gibi amaçlarla kendi imza oluşturma verisini saklayabilir, ancak Elektronik İmza Kanunu'nun 10. maddesi doğrultusunda sertifika sahiplerinin imza oluşturma verilerini yedekleyemez ve imza oluşturma verisi kurtarma hizmeti veremez.

[62] European Commission, Certıficate Practıce Statement, Version 1.0, February 2002 s. 31

5. Tesis, Yönetim ve Operasyonel Kontroller (Management, Operational, and Physical Controls)

Bu bölümde ESHS'nin işlevini yerine getirirken uyguladığı temel fiziksel ve operasyonel kontroller ve prosedürler açıklanmaktadır.

5.1. Fiziksel Kontroller (Physical Security Controls)

ESHS, nitelikli elektronik sertifika yaşam zinciri operasyonları ve anahtar yönetimi de dahil olmak üzere temel ESHS operasyonlarının tümünü gizli veya açık müdahaleleri durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan bir "Güven Merkezi" içinde yürütmelidir[63]. Güven Merkezi ve ESHS'nin temel ESHS operasyonlarında kullanılan donanımlar, 7/24 operasyonlarına devam edebilmeleri için kesintisiz güç kaynakları ile; sıcaklığı ve nispi nemi kontrol etmek için ise ısıtma/havalandırma/klima sistemleri ile, su baskınları ve sele karşı binanın üst katında inşaa edilmiş ve gerekli yalıtım sistemleri ile, yangına karşı gerekli söndürme sistemleri ile donatılmalıdır.

5.2. Prosedür Kontrolleri (Procedural Controls)

Nitelikli elektronik sertifika yaşam zinciri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, ESHS yönetim sistemleri ve veri bankaları kontrolleri, gerekli erişim ve kontrol yetkisine sahip "güvenli personel" tarafından yürütülmelidir. Güvenli personel elektronik imza teknolojisi, bilgi güvenliği ve risk yönetimi konularında yeterli bilgi ve tecrübe

[63] ESnet Root CA Certificate Policy And Certification Practice Statement, Version 1.0, January 2003 s.12

seviyesine sahip kişilerden seçilmelidir. ETSI TS 101 456 ile belirlenen güvenli personel tanımları aşağıdaki şekildedir[64];

- Güvenlik Yöneticileri: Güvenlik sistemininin tüm politika ve prensiplerinin belirlenmesi, uygulanması, onaylanması görev, yetki ve sorumluluğuna sahip güvenli personel

- Sistem Yöneticileri : nitelikli elektronik sertifika başvuruları yönetimi, nitelikli elektronik sertifika oluşturulması, güvenli elektronik imza oluşturma araçları yönetimi, sertifika iptal yönetimi için kullanılan ESHS güvenli sistemlerini kurma, konfigüre etme ve bakımını yapma görev ve yetkisine sahip güvenli personel

- Sistem Operatörleri : ESHS güvenli sistemlerini günlük bazda kullanma, sistem yedeklemesi ve kurtarma fonksiyonlarını kullanma görev ve yetkisine sahip güvenli personel

- Sistem Denetçileri : ESHS güvenli sistemlerinin denetim kayıtlarına ve arşivlerine erişme ve devamlılığını sağlama görev ve yetkisine sahip güvenli personel

Bazı nitelikli elektronik sertifika sertifika yaşam zinciri işlemleri, ESHS anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok güvenli personelin katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilmelidir.

[64] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s. 29

5.3. Personel Kontrolleri (Personal Controls)

ESHS'nin, kurucu ortakları, tüzel kişiliği temsile yetkili yöneticileri ve istihdam ettiği veya ettirdiği personeli - taksirli suçlar hariç olmak üzere - affa uğramış olsalar bile ağır hapis veya altı (6) aydan fazla hapis yahut basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, 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 olacaktır[65].

ESHS personeli göreve başlamadan önce ESHS hizmetleri, sertifika yaşam zinciri hizmetleri, mesleki sorumluluklar, temel açık anahtar alt yapısı çerçevesi, ESHS güvenlik prosedürleri ve sertifika politikaları konularında gerekli hukuki ve teknik eğitimden geçirilmelidir. ESHS, ESHS faaliyetlerini yürütmek için bağımsız yükleniciler ile hizmet sözleşmeleri akdedebilir. Hizmet sözleşmeleri ESHSnın güvenlik ve işleyiş süreçlerine uyumlu olacak şekilde düzenlenir.

5.4. Denetim ve Kayıt Prosedürleri (Audit Logging Procedures)

ESHSnın ESHS işleyişine ve organizasyonel fonksiyonlarına ilişkin aşağıdaki kayıtlar elektronik ve/veya kağıt ortamında - olayın tanımı, gerçekleşme tarihi, olayla ilgili kişilere ilişkin bilgiler de dahil olmak üzere - tutulur[66].

- ESHS anahtar (veri) yaratma, yedekleme, saklama, kurtarma, arşivleme ve imha etme.
- Şifreleme cihazı periyodu yönetimi olayları.
- nitelikli elektronik sertifika başvuruları, yenileme, yeniden anahtarlama ve iptal.

[65] e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları, Kasım 2005 s.47
[66] Comodo Group, Comodo Certification Practice Statement, April 2003 s. 31

- Sertifikaların ve SİL'lerin yaratılması ve yayınlanması.
- Başarılı veya başarısız sisteme erişim girişimleri.
- Sistem arızaları, donanım arızaları ve diğer anormallikler.
- Güvenlik duvarı ve rooter aktivitesi.
- ESHS operasyon merkezi tesisi ziyaretçi girişi/çıkışı

Denetim kayıtları sürekli olarak tutulur ve en azından haftada bir olmak üzere belirli zaman aralıklarıyla incelenir. Denetim kayıtları - en az haftada bir kere olmak üzere - yedeklenir ve arşivlenir. Denetim kayıtları işlendikten sonra veri depolama kapasitesine göre erişilebilir şekilde sistemde tutulur.

Elektronik ve kağıt ortamındaki denetim kaydı dosyalarına, yetkisiz kişilerin izlemesine, değişiklikler yapmasına, silmesine veya başka herhangi bir şekilde erişmesine karşı fiziksel ve mantıksal erişim kontrolleri kullanılır ve bu yolla denetim kaydı dosyaları korunur.

5.5. Kayıtların Arşivlenmesi (Records Archival)

ESHS, denetim kayıtlarına ilave olarak nitelikli elektronik sertifika başvuruları ile sertifika sahipleri, ESHS ve diğer katılımcılar arasındaki bütün veri iletişimine ilişkin kayıtları tutar[67]. Arşivde bulunan belgeler saklanma süresi boyunca okunabilir bir formatta tutulmalıdır. Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 14. maddesine göre ESHS,

a) Geçerlilik süresi sona eren nitelikli elektronik sertifikaları,

b) Nitelikli elektronik sertifika başvurusunda talep edilen bilgi, belge ve elektronik verileri,

[67] Information Security Committee Electronic Commerce and Information Technology Division, Digital Signature Guidelines, American Bar Association, August 1996 s. 83

c) Sertifika ilkelerini ve sertifika uygulama esaslarını,

d) Zaman damgası ilkelerini ve zaman damgası uygulama esaslarını,

e) Geçerlilik süresinin sona ermesinden itibaren kendi sertifikasını,

f) Nitelikli elektronik sertifika yönetimine ilişkin tüm işlemlere, bu işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kaydı,

en az yirmi (20) yıl süreyle saklar.

5.6. İmza Oluşturma – Doğrulama Verileri (Anahtar) Değiştirme (Key Changeover)

ESHS imza oluşturma ve doğrulama verilerinin geçerlilik süreleri, mevzuatta belirtildiği üzere, en fazla 10 yıl olmalıdır. Gerekli görülen durumlarda güvenlik sebebiyle ve ESHS imza oluşturma verisinin geçerlilik süresinin dolmasından önce ESHS imza oluşturma verisi yenilenir. Bu durumda eski imza oluşturma ve doğrulama verileri geçerlilik süresinin sonuna kadar kullanılabilir durumda saklanmalıdır.

5.7. Tehlike ve Felaketten Kurtarma (Compromise and Disaster Recovery)

ESHS işleyişinin güvenilirliğini etkileyecek nitelikte olayların oluşması durumunda "İş Sürekliliği ve Felaketten Kurtarma Planı" doğrultusunda sistemin en kısa sürede güvenli bir şekilde işler hale gelmesi, etkilenen taraflara haber verilmesi ve diğer önlemlerin uygulanması için gerekli önlemler alınır[68].

[68] ETSI TS 101 456, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006 s. 33

Güven Merkezinde bulunan donanım, yazılım ve gerekli verilerin bozulması halinde öncelikle yedek donanım ve yazılım faaliyete geçirilir. İş Sürekliliği ve Felaketten Kurtarma Planı doğrultusunda kaybolan verilerin yedekleri işleme konulur ve/veya yeniden oluşturulur. Kurtarılamayan veriler sebebiyle sertifika yönetim süreçlerinde geri dönülemez arızalar meydana gelmesi halinde, arızadan etkilenen sertifikalar derhal iptal edilir ve ilgili taraflara bilgi verilir.

ESHS kök sertifikalarının imza oluşturma verilerinin güvenliğinin tehlikeye düşmesi durumunda İş Sürekliliği ve Felaketten Kurtarma Planı doğrultusunda ilgili tüm sertifikalar derhal iptal edilir ve ilgili tüm taraflar web sitesi ve e-posta aracılığıyla haberdar edilir. ESHS kök sertifikalarının yeni imza oluşturma verileri oluşturulur.

5.8. ESHS'nin veya Kayıt Merkezi'nin Operasyonunun Durdurulması (CA or RA Termnation)

ESHS "kayıt merkezleri"nin operasyonlarının durdurulması halinde "kayıt merkezi"nde tutulan tüm bilgi ve belgeler "Güven Merkezi"ne taşınır ve/veya imha edilir. ESHS, faaliyetlerini durdurması gerektiği durumlarda, ESHS operasyonları durdurulmadan önce sertifika kullanıcılarını, kurumsal başvuru sahiplerini, üçüncü kişileri ve diğer ilgili kuruluşları bundan haberdar etmek için ticari açıdan gerekli her türlü çabayı gösterir[69].

Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında "Yönetmelik"in 29. maddesine göre;

Telekomünikasyon Kurumu, yaptığı denetim sonucunda, ESHS'nin, faaliyetinin devamı sırasında bildirim şartlarından birini veya birkaçını kaybettiğini tespit etmesi halinde ESHS'ye bu eksikliğin giderilmesi için bir (1) aya kadar süre verir ve bu süre içinde ESHS'nin faaliyetini durdurur. Telekomünikasyon Kurumu, vermiş

[69] VeriSign Trust Network European Directive Supplemental Policies, Version 1.0, September 19, 2001 s. 36

olduğu sürenin sonunda eksikliğin giderilmemesi veya Kanunun 18 inci maddesindeki suçların işlendiği tarihten itibaren geriye doğru üç (3) yıl içinde üçüncü kez işlenmiş olması halinde ESHSnin faaliyetine son verir.

Yukarıda bahsedilen faaliyete son verme hallerinden birinin gerçekleşmesi ile faaliyetine son verilen ESHS, faaliyete son verme kararının tebliği tarihinden itibaren on beş (15) gün içinde faaliyette bulunan herhangi bir ESHS ile nitelikli elektronik sertifikaların devri konusunda anlaşabilir. Telekomünikasyon Kurumu, taraflar arasında anlaşma sağlanması durumunda, faaliyetine son verilen ESHS'nin oluşturduğu nitelikli elektronik sertifikaların anlaşma sağlanan ESHS'ye devredilmesine karar verir. Faaliyetine son verilen ESHS ile faaliyette bulunan herhangi bir ESHS arasında onbeş (15) gün içinde nitelikli elektronik sertifikaların devrine ilişkin anlaşma sağlanamaması durumunda Telekomünikasyon Kurumu, nitelikli elektronik sertifikaların herhangi bir ESHS'ye devrine re'sen karar verir. Nitelikli elektronik sertifikaları devralan ESHS sertifika yenileme işlemlerini başlatır ve devir kararının tebliği tarihinden itibaren bir (1) ay içinde bu işlemleri tamamlar. Telekomünikasyon Kurumu, uygun görmesi halinde, bir (1) ayı geçmemek üzere ek süre verebilir.

ESHS, Telekomünikasyon Kurumu'nun faaliyete son verme kararının tebliğinden itibaren elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayamaz. Ancak, sertifika yenileme işlemleri tamamlanıncaya kadar iptal durum kaydı hizmetini devam ettirir.

Faaliyetine son verilen ESHS, nitelikli elektronik sertifikalari devralan ESHSye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devreder ve kendi imza oluşturma verisi ile yedeklerini imha eder.

Telekomünikasyon Kurumu, nitelikli elektronik sertifikalari re'sen devredebileceği herhangi bir ESHSnin bulunmaması durumunda, faaliyetine son verdiği ESHSnin oluşturduğu nitelikli elektronik sertifikaların iptal edilmesine karar verir. Faaliyetine son verilen ESHS son iptal durum kaydını oluşturduktan sonra kendi imza

oluşturma verisi ile yedeklerini imha eder, geçerlilik süresi en geç sona eren nitelikli elektronik sertifikanın geçerlilik süresi sonuna kadar, iptal durum kaydı hizmetini devam ettirir ve arşivi en az yirmi (20) yıl süreyle saklar.

Kurum, nitelikli elektronik sertifikaların devrine ilişkin kararları internet sayfasında yayımlar. Faaliyetine son verilen ESHS devire ilişkin kararları nitelikli elektronik sertifika sahiplerine elektronik posta ile duyurur ve internet sayfasında yayımlar.

Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında "Yönetmelik"in 30. maddesine göre;

ESHS faaliyetine son vereceği tarihten en az üç (3) ay önce durumu Kuruma yazılı olarak bildirir. ESHS, faaliyetine son verme kararının Kuruma bildirilmesinden itibaren nitelikli elektronik sertifika başvurusu kabul edemez ve yeni nitelikli elektronik sertifika oluşturamaz.

ESHS faaliyetine son vereceği tarihten en az üç (3) ay önce faaliyetine son verme kararını internet sayfasında yayımlar, sertifika sahiplerine elektronik posta ile bildirir ve ulusal yayın yapan en yüksek tirajlı üç (3) gazetede ilan vermek suretiyle kamuoyuna duyurur.

ESHS, faaliyetine son verme tarihine kadar geçerlilik süresi sona ermeyecek ve kullanımı faaliyette bulunan herhangi bir ESHS tarafından sağlanabilecek nitelikli elektronik sertifikaları, faaliyete son verme tarihinden bir (1) ay öncesine kadar faaliyette bulunan herhangi bir ESHS'ye devredebilir. Faaliyetine son veren ESHS devir hususunda sertifika sahiplerini elektronik posta ile bilgilendirir. Nitelikli elektronik sertifikaların devredilmesi halinde sertifikaları devralan ESHS sertifika yenileme işlemlerini başlatır ve bir (1) ay içinde bu işlemleri tamamlar. Kurum, uygun görmesi halinde, bir (1) ayı geçmemek üzere ek süre verebilir.

Nitelikli elektronik sertifikaları devreden ESHS, sertifikaları devralan ESHSye kimlik doğrulamada kullanılan belgeleri, dizini, arşivi ve sertifika yenileme işlemlerinin tamamlanmasından sonra iptal durum kaydını devreder ve kendi imza oluşturma verisi ile yedeklerini imha eder.

Faaliyetine son verme tarihinden bir (1) ay öncesine kadar nitelikli elektronik sertifikaların devredilememesi veya nitelikli elektronik sertifikaların kullanımının faaliyette bulunan herhangi bir ESHS tarafından sağlanamaması durumunda, faaliyetine son vermek isteyen ESHS nitelikli elektronik sertifikaları faaliyete son verme tarihinde iptal eder. Faaliyetine son veren ESHS son iptal durum kaydını oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder, geçerlilik süresi en geç sona eren nitelikli elektronik sertifikanın geçerlilik süresi sonuna kadar iptal durum kaydı hizmetini devam ettirir ve arşivi en az yirmi (20) yıl süreyle saklar.

6. Teknik Güvenlik Kontrolleri (Technical Security Controls)

6.1. İmza Oluşturma ve Doğrulama Verilerini Oluşturma ve Kurma (Key Pair Generation and Installation)

ESHS imza oluşturma ve doğrulama verileri oluşturma işlemi, oluşturulan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş birden fazla eğitimli "güvenli personel" ve ilgili görevliler tarafından yerine getirilir[70]. ESHS kök sertifikası için, imza oluşturma ve doğrulama verileri oluşturmada kullanılan şifreleme modülleri FIPS 140-1 Seviye 3 şartlarını karşılamalıdır[71]. ESHS kök sertifikasının imza oluşturma ve doğrulama verileri Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritmalara ve standartlara uygun olarak oluşturulur; anahtar oluşturma işlemi

[70] Dexia Root CA Certification Practice Statement, Version 1.0, s. 34

[71] Identrus Identity Certificate Policy IP-ICP Version 2.0, 2003 s. 8

sırasında yapılan faaliyetler kaydedilir, tarih atılarak imzalanır. Bu kayıtlar denetim ve izleme amacıyla saklanır. İmza oluşturma verisi ESHS'nin güvenli elektronik imza oluşturma aracında oluşturulur ve buradan yedekleme amacı dışında çıkarılamaz. İmza oluşturma verisinin güvenli olarak saklanması için gerekli fiziksel ve teknik güvenlik önlemleri alınır. ESHS sertifikalarına (kök ve alt kök sertifikalar) ait özet Türkiye'de yayımlanan en yüksek tirajlı üç ulusal gazetede kamuoyuna duyurulur.

Nitelikli elektronik sertifikanın imza oluşturma ve doğrulama verileri sadece güvenli elektronik imza oluşturma ve doğrulama amacıyla kullanılır. ESHS kök sertifikası imza oluşturma ve doğrulama verileri ise nitelikli elektronik sertifika imzalama, sertifika iptal listesi imzalama, çevrimiçi sertifika durum protokolü sertifikası imzalama, zaman damgası sertifikası imzalama amaçlarıyla kullanılabilirler.

6.2. İmza Oluşturma Verisinin Korunması ve Şifreleme Modülü Sistem Kontrolleri (Private Key Protection and Cryptographic Module Engineering Controls)

ESHS kök sertifikasının imza oluşturma, doğrulama verilerini oluşturma ve imza oluşturma verisi saklama işlemleri için FIPS 140-1 Seviye 3'de yetkili onaylanmış donanım şifreleme modülleri kullanılır. ESHS kök sertifikaları yedekleme, felaketten kurtarma ve iş sürekliliğinin sağlanması amaçlarıyla parçalara bölünüp farklı lokasyonlarda saklanır; bu lokasyona erişim bilgileri/şifreleri sadece birden çok güvenilir personele veya denk ilgili kişilere saklamaları için teslim edilir[72].

Nitelikli elektronik sertifika sahiplerine ait imza oluşturma verileri güvenli elektronik imza oluşturma araçlarında oluşturulur ve oluşturuldukları güvenli elektronik imza oluşturma aracı dışarısına kesinlikle çıkarılamaz.

[72] CNRS/CNRS-Projets/Datagrid-fr, Certificate Policy and Certification Practice Statement, Version 0.3, August 2002 s.10

6.3. Anahtar Çifti Yönetiminin Diğer Yönleri (Other Aspects of Key Pair Management)

ESHS kök sertifikaları, nitelikli elektronik sertifikalar ve bunlara bağlı imza doğrulama verileri en az 20 yıl boyunca saklanır. Saklama süresince verilerin bütünlüğü sağlanması için gereken her türlü önlem alınır.

6.4. Aktivasyon Verileri (Activation Data)

Aktivasyon verileri, ESHS'nin personelinin teknik güvenlik gerektiren işlemlerde kullandığı şifreler ve erişim verileri ile nitelikli elektronik sertifika sahiplerinin güvenli elektronik imza oluşturma araçlarına erişim için kullandıkları şifrelerdir.

Aktivasyon verilerinin nitelikli elektronik sertifika sahiplerine ve personele iletilmesinden sonra, verilerin gizliliğinin ve güvenliliğinin korunmasıyla ilgili sorumluluk nitelikli elektronik sertifika sahiplerine ve personele aittir.

6.5. Bilgisayar Güvenlik Kontrolleri (Computer Security Controls)

ESHS bilgi güvenliği gereksinimleri, güvenli ve lisanslı yazılım ve donanımların kullanılması, ağ içerisinde saldırı tespit sistemlerinin bulunması, bilgi ve zilyetlik bazlı tanımlama yöntemleri ile erişim ve işlem kontrolü, "güvenli personel" arasında münhasır yetki ve görev dağılımı, gerekli tüm işlemlerin ve kayıtların yedeklenmesi ve saklanması yöntemleri ile sağlanmalıdır.

6.6. Yaşam Zinciri Teknik Kontrolleri (Lifecycle Technical Contols)

ESHS sertifika yaşam zinciri sistem geliştirme kontrolleri ESHS kalite yönetimi prosedürleri ve TS "17799-2 denetimleri sonucunda ortaya çıkan risk azaltma metodları uyarınca gerçekleştirilmelidir.

6.7. Ağ Güvenlik Kontrolleri (Network Security Controls)

ESHS'nin güven merkezinin anahtar üretimi, sertifika yaşam döngüsü kontrolleri ve diğer sistemleri gerekli ağ güvenliği alt yapısına sahip olmalıdır.

6.8. Zaman Damgası (Time Stamps)

ESHS sunduğu zaman damgası hizmetlerine ilişkin bilgileri bu bölümde bildirir; veya doğrudan Zamana Damgası İlkeleri ve Zaman Damgası Uygulama Esasları Dokümanları'na atıf yapar.

7. Sertifika ve Sertifika İptal Listesi Profilleri (Certificate and CRL Profiles)

7.1. Sertifika Profili (Certificate Profile)

Nitelikli elektronik sertifikalar ITU-TRec X.509V.3 (1997), RFC 3280 ve ETSI TS 101 862 standartlarına uygun olmak zorundadır. ESHS kök sertifikalarında ve nitelikli elektronik sertifikalarda X.509V.3 (1997) ve ETSI TS 101 862 de desteklenen bütün uzantılar kullanılabilir. Nitelikli elektronik sertifikaların anahtar kullanım alanları uzantılarında sadece inkar edilemezlik (non-repudiation) ve dijital imza (digital signature) uzantılarının kullanılmasına izin verilir. ESHS kök sertifikalarında ise anahtar kullanım uzantılarında sertifika imzalama (KeyCertSign), "SİL" imzalama (CRLSign), çevrimdışı "SİL" imzalama (off-line CRLSign) uzantıları kullanılır.

Nitelikli elektronik sertifikalarda anonim veya takma adlar kullanılamaz; adların tekliğini sağlamak için T.C. kimlik numarası kullanılır. Nitelikli elektronik sertifikalar, sertifika ilkeleri ve nitelikli sertifika ibaresi için sertifika politikası nesne belirteci ("OID") içerir. Nitelikli elektronik sertifikaların sertifika ilkeleri uzantısında "SUE"ye erişimi sağlayan bir "URL" bulunur. Nitelikli elektronik sertifikaların sertifika ilkeleri uzantısında, ESHS'ye ait TSE'den tahsis edilmiş nesne belirteci altında söz konusu ESHS için belirlenen nesne belirteci kullanılır. Nitelikli elektronik sertifikaların sertifika ilkeleri uzantısında, ETSI TS 101 456 QC+SSCD Policy uyumluluk için ilgili nesne belirteci kullanılır.

ESHS tarafından yayınlanan Nitelikli elektronik sertifikanın nitelikli elektronik sertifika olduğuna dair bir ibare Qc Statements-Statement ID altında "Bu sertifika 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır" şeklinde yer alır. Nitelikli elektronik sertifikaların sertifika ilkeleri uzantısında opsiyonel olarak ilgili oldukları imzalama ilkelerine (signature policy) ait nesne belirteci bulunabilir.

7.2. Sertifika İptal Listesi Profili (CRL Profile)

Sertifika iptal listelerinde ESHS sertifikası ile atılmış elektronik imza, sertifika iptal listesinin yayınlanma tarihi, bir sonraki sertifika iptal listesinin yayınlanma tarihi, iptal edilen nitelikli elektronik sertifikaların seri numaraları ve iptal edilme zamanı yer alır[73].

7.3. Çevrimiçi Sertifika Durum Protokolü Profili (OCSP Profile)

Çevrimiçi sertifika durum protokolü gerçek zamanlı nitelikli elektronik sertifika sorgusu hizmetidir. ESHS çevrimiçi sertifika durum protokolü hizmetinde RFC 2560 gerekliliklerine uymalıdır.

[73] SUN Public Key Infrastructure Certification Practice Statement, Version 1.52, November 2000 s.10

8. Uyum Denetimi ve Diğer Değerlendirmeler (Compliance Audit and Other Assessment)

ESHS mevzuat gereğince Telekomünikasyon Kurumu'nun denetimine tabidir. ESHS ayrıca TST 17799-2 sertifikası gereğince bilgi güvenliği açısından periyodik denetimlere tabi tutulur. Telekomünikasyon Kurumu tarafından yapılan denetimlerin sıklığı, Kurum yetkililerinin inisiyatifinde olmakla beraber, en az iki yılda bir yapılacaktır. Diğer denetimlerin sıklığı ESHS'nin bağlı olduğu bilgi güvenliği sistemleri doğrultusunda belirlenecektir.

Telekomünikasyon Kurumu tarafından yapılan denetimler yetkili Kurum personeli tarafından yapılır. Diğer denetimler ESHS'nin bağlı olduğu bilgi güvenliği sisteminin yetkili denetçileri tarafından, iç denetimler ise ESHS'nin yetkili personeli tarafından yapılacaktır. Telekomünikasyon Kurumu tarafından yapılan değerlendirme, ESHS'nin alt yapınsın ve işleyişinin ilgili mevzuata, mevzuatla belirlenen uluslararası standartlara ve kendi sertifika ilkeleri ve sertifika uygulama esaslarına uygun olup olmadığına ilişkindir. Diğer denetimler ESHS'nin bağlı olduğu bilgi güvenliği sisteminin kapsamına göre belirlenir.

Telekomünikasyon Kurumu tarafından yapılan denetimlerde ESHS'nin mevzuattan ve ilgili standartlardan doğan yükümlülüklerini yerine getirmemesi durumunda mevzuatta öngörülen yaptırım ve cezalar uygulanacaktır. ESHS kendi iç denetimlerinde eksiklerini gidermek için bir prosedür hazırlamalıdır.

9. Diğer Ticari ve Hukuki Konular (Other Business and Legal Matters)

9.1. Ücretler (Fees)

Bu bölümde ESHS, nitelikli elektronik sertifikalara ve diğer hizmetlerine ilişkin ücret ve geri ödeme politikasını belirtir. ESHS nitelikli elektronik sertifika iptal ve durum erişim hizmetleri için ücret talep edemez.

9.2. Finansal Sorumluluklar (Financial Responsibility)

ESHS Elektronik İmza Kanunu'nun 13.maddesine göre zorunlu sertifika mali sorumluluk sigortası yaptırmak zorundadırlar. Zorunlu sertifika mali sorumluluk sigortası:

- ESHS'nin güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek, sertifikaların taklit ve tahrif edilmesini önlemek ile ilgili görevlerini gerektiği biçimde yerine getirmemesi,

- Sertifikaların içeriğinde ESHS'den kaynaklanan yanlış bilgilerin bulunması,

- Sertifikaların oluşturulması sırasında nitelikli elektronik imza sahiplerinin verdikleri bilgilerin ESHS tarafından eksik veya yanlış işlenmesi sonucu ortaya çıkan hataların bulunması,
- Sertifikaların ESHS ile nitelikli elektronik sertifika sahipleri arasında yapılan sözleşmeye tam ve uygun olarak hazırlanmaması,

gibi ESHS'nin ve eylemlerinden sorumlu bulunduğu personelin kusurundan, ihmalinden veya gerekli özeni göstermemesinden doğan maddi zararları kapsar.

Aşağıdaki hallerden birinin veya birkaçının sonucunda doğan sorumluluğa bağlı olarak;

- Savaş, düşman hareketleri, çarpışma (savaş ilan edilmiş olsun veya olmasın), ihtilal, ayaklanma ve bunların gerektirdiği inzibati askeri hareketlerden,

- Herhangi bir nükleer yakıttan veya nükleer yakıtın yanması sonucu nükleer atıklardan veya bunlara atfedilen sebeplerden meydana gelen iyonlayıcı radyasyonlar veya radyo-aktivite bulaşmaları ve bunların gerektirdiği inzibati ve askeri tedbirlerden,

- Deprem, yanardağ püskürmesi, deniz depremi, sel, seylap ve su baskını, yer kayması gibi doğal afetlerden,

- Kamu otoritesi tarafından yapılacak tasarruflar sonucunda oluşan ve ESHS'nin kusurundan kaynaklanmayan sorunlardan,

- İletişim altyapısı ve ESHS'nin doğrudan kontrolü altında olmayan bilgi işlem altyapısında meydana gelen sorunlardan,

- İmza sahibi tarafından kanun dışı amaçlar için nitelikli elektronik imzanın kullanılmasından,

- Sigortacıya veya sigorta ettirene haber verildikten sonraki bir tarihte ESHS tarafından iptal edilmeyip ikinci veya daha çok miktarda hasar oluşmasına neden olan aynı nitelikli elektronik sertifika ile işlem yapılmasından,

- Faaliyet konusu ile ilgili kanun, yönetmelik ve tebliğlerle belirlenen esaslar ve teknik standartlara bağlı kalınmamasından,

doğan zararlar sigorta teminatı dışındadır[74].

9.3. Ticari Bilgilerin Gizliliği（Confidentiality of Business Information)

ESHS'nin teknik ve operasyonel anlamda işlemlerine ilişkin bilgi güvenliği kapsamında gizli sayılan tüm bilgi ve belgeler, ESHS'nin ticari faaliyetlerine ilişkin her türlü gizli bilgi ve belge, ESHS kök ve alt kök sertifikaları imza oluşturma verileri, işlem kayıtları, nitelikli elektronik sertifika sahiplerinin mevzuat kapsamında kişisel veri sayılan bilgileri, denetim ve değerlendirme kayıtları, güven merkezi ile ilgili her türlü gizli bilgi ve belge, donanım ve yazılımla ilgili teknik güvenlik bilgileri gizli bilgi kapsamındadır.

9.4. Kişisel Bilgilerin Mahremiyeti (Privacy of Personal Information)

Elektronik İmza Kanunu'nun 12. maddesine göre ESHS;

1.

- Nitelikli elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

- Nitelikli elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

- Nitelikli elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri nitelikli elektronik sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

[74] Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları

9.5. Fikri Mülkiyet Hakları (Intellectual Property Rights)

ESHS bu bölümde, kendi markasına, yayınladığı dokümanlara ve sertifikalara, kullandığı yazılımlara ilişkin fikri ve sınai haklar hakkında bilgi verir.

9.6. Sorumluluk ve Garantiler (Representations and Warranties)

ESHS'lere sorumluluk rejimleri "Kanun"un 13. maddesine tabi olup, bu maddeye göre ESHS'nin sertifika sahibine karşı sorumluluğu genel hükümlere göre belirlenecektir. ESHS, mevzuat hükümlerinin ihlâli suretiyle üçüncü kişilerin zararına sebebiyet verecek olursa bu zararı tazminle mükelleftir. Mevzuat hükümlerinin ihlâli suretiyle üçüncü kişilerin zararına sebebiyet verecek durumun ESHS'nin istihdam ettiği kişilerin davranışa dayanması sonucunda da ESHS bu zarardan sorumlu olup, ESHS bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz. ESHS nitelikli elektronik sertifika sahiplerine ve üçüncü kişilere karşı sorumluluğunu ancak nitelikli elektronik sertifikanın kullanım ve maddi kapsama ilişkin sınırlamaları anlamında kısıtlayabilir. ESHS, nitelikli elektronik sertifikanın içerisinde belirtilen maddi kapsama ve/veya kullanıma ilişkin sınırlamaların dışında kullanılması durumunda, bu sınırlama dışı kullanımlardan dolayı doğacak zararları tazminle mükellef olmayacaktır. ESHS, mevzuattan doğan yükümlülüklerini yerine getirmemesi sonucu ortaya çıkacak zararların karşılanması amacıyla Kanunun 13.maddesinde belirtilen zorunlu sertifika malî sorumluluk sigortasını yaptırmak zorundadır.

Nitelikli elektronik sertifika sahibi, kullanımdan önce Nitelikli elektronik sertifikanın geçerlilik durumunu kontrol etmekle, geçerliliği sona ermiş, askıda bulunan veya iptal edilmiş Nitelikli elektronik sertifikayı kullanmamakla, Nitelikli elektronik sertifikayı sadece güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanmakla, kendisine ait olan imza oluşturma verisini kimseye kullandırmamakla, aktivasyon verisinin gizliliğini sağlamakla, nitelikli elektronik sertifikanın kullanım ve maddi kapsama ilişkin sınırlar dahilinde kullanmakla, nitelikli elektronik sertifikayı kullandığı ortamların gizliliğini ve güvenliğini sağlamakla, nitelikli elektronik

sertifikayı imzalamış olduğu kullanıcı sözleşmesine, sertifika uygulama esaslarına ve sertifika ilkelerine uygun olarak ve hukuka uygun amaçlarla kullanmakla, başvuru süreçlerinde ESHS personeline doğru, geçerli ve yeterli bilgi ve belgeleri sağlamakla yükümlüdür.

Üçüncü kişiler nitelikli elektronik sertifika ile ilişkili olarak oluşturulmuş bir güvenli elektronik imzaya güvenerek herhangi bir iş veya işlem yapmadan önce güvenli elektronik imzayı doğrulamakla ve nitelikli elektronik sertifikanın geçerliliğini kontrol etmekle yükümlüdürler[75]. Üçüncü taraflar bu sorumluluklarını "güvenli elektronik imza doğrulama aracı" kullanarak yerine getirebilirler. Üçüncü kişiler aynı zamanda Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik 16. Maddesinde belirtilen yükümlülüklere uymakla mükelleflerdir.

ESHS üçüncü taraflarla bazı hizmetlerin görülmesi için hizmet sözleşmeleri yapabilir. Bu üçüncü tarafların sorumlulukları kendileriyle yapılan hizmet sözleşmeleri uyarınca belirlenir.

9.7. Garantilerin Reddi (Disclaimers of Warranties)

ESHS, katılımcıların sertifika ilkelerine, sertifika uygulama esaslarına, imzaladıkları sözleşmelere uymamaları ve mevzuattan doğan yükümlülüklerini yerine getirmemeleri şartıyla garantilerin reddiyle ilgili hükümler belirleyebilir.

9.8. Sorumluluğun Sınırlandırılması (Limitations of Liability)

Elektronik İmza Kanunu'nun 13. maddesine göre ESHSlerin sorumlulukları yalnızca Nitelikli elektronik sertifikada bulunan kullanım ve maddi kapsama ilişkin sınırlamalar ile sınırlandırılabilir.

[75] CERN Certification Authority, Certificate Policy and Certification Practice Statement, Draft Version 1.1, April 2003 s. 11

9.9. Tazminatlar (Indemnities)

Bu bölümde ilgili tarafların, sertifika ilkelerine, sertifika uygulama esaslarına, imzaladıkları sözleşmelere uymamaları ve mevzuattan doğan yükümlülüklerini yerine getirmemeleri halinde ortaya çıkan tazminat yükümlülükleri ile ilgili bilgiler verilmektedir.

9.10. Geçerlilik ve Sona Erme (Term and Termination)

Bu bölümde sertifika ilkeleri ve sertifika uygulama esaslarının, geçerlilik tarihleri, sona erme halinde uygulanacak olan kurallar ve yeni versiyonların yürürülüğe girme tarihleri hakkında bilgi verilir.

9.11. Bireysel Mesajlar ve Katılımcılarla İletişim (Individual notices and communications with participants)

Bu bölümde sertifika ilkeleri ve/veya sertifika uygulama esaslarının kapsamına giren katılımcılar arasındaki birebir iletişim hangi koşullarda gerçekleşebileceği ve buna ilişkin yasal zemin hakkında bilgi verilir.

9.12. Değişiklikler (Amendments)

Bu kısımda ise sertifika ilkeleri ve/veya sertifika uygulama esasları dokümanlarında değişikliğin hangi koşullarda yapılabileceği, katılımcılardan gelen taleplerin değişiklik olarak dokümanlara yansıtılma prosedürü ve değişikliğin geçerli hale gelme koşulları anlatılır. ESHS'ler sertifika ilkeleri veya sertifika uyulama esaslarında yaptıkları değişiklikleri 7 (yedi) gün içerisinde Telekomünikasyon Kurumu'na bildirmelidir.

9.13. Uyuşmazlık Çözüm Yolları (Dispute Resolution Procedures)

Elektronik İmza Kanunu'nun 10 maddesinin e bendine göre ESHS'nin "*Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle*" ilgili yükümlülüğü bulunmaktadır. Maddede belirtilen uyuşmazlık çözüm yolları bu başlık altında belirlenebilir. Söz konusu uyuşmazlık çözüm yolları sulh ve tahkim gibi alternatif uyuşmazlık çözüm yolları arasından belirlenmelidir.

9.14. Uygulanacak Hukuk (Governing Law)

Bu bölümde sertifika ilkeleri ve/veya sertifika uygulama esasları ile ilgili bir uyuşmazlık ortaya çıktığında, uyuşmazlığın yorumlanmasında hangi ülke hukukunun kullanılacağı belirlenmektedir.

9.15. Mevzuata Uyumluluk (Compliance with Applicable Law)

ESHS'lerin yayınladığı sertifika ilkeleri ve sertifika uygulama esaslarının, 5070 sayılı Elektronik İmza Kanunu, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ve Tebliğ ile belirlenen uluslararası standartlara uygun olması gerekmektedir.

9.16. Çeşitli Hükümler (Miscellaneous Provisions)

Bu bölümde, sertifika ilkeleri ve sertifika uygulama esaslarının bir sözleşm kurgusu içerisinde olduğu düşünülerek, bütünlük, mücbir sebep, bölünebilirlik, devir ve temlik gibi sözleşmelerde kullanılan genel hükümlere yer verilir.

C. ZAMAN DAMGASI İLKELERİ VE ZAMAN DAMGASI UYGULAMA ESASLARI

Zaman damgası ilkeleri ve zaman damgası uygulama esasları, zaman damgası hizmetlerine ilişkin detaylı açıklamaların yapıldığı, şart ve koşulların belirlendiği dokümanlardır[76]. Esas olarak sertifika ilkeleri ve sertifika uygulama esaslarıyla aynı işleve sahip olmakla birlikte, sertifikaya değil zaman damgasına ilişkin çerçeveyi çizmektedirler. Bunu dışında her iki doküman seti arasında içerik, oluşturulma ve yayınlanma prosedürü, katılımcılar, hukuki statü gibi konularda bir farklılık yoktur. Yurtdışı uygulamalarına bakıldığında da zaman damgası hizmetleri için ayrı ilke ve uygulama esaslarının yaratılmadığı görülmektedir. RFC 3647 sertifika ilkeleri ve sertifika uygulama esasları çerçevesinde de bir bölüm zaman damgası hizmetlerine ayrılmıştır.

Ancak, Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), Avrupa Elektronik İmza Standardizasyon İnisiyatifi içerisinde öngördüğü elektronik imza yapısı içerisinde, elektronik imza hizmetlerinin birbirinden ayrı olarak sunulabileceğini belirtmiştir. Kanaatimizce bu sebepten ötürü zaman damgası hizmetleri için de ayrı bir ilke çerçevesi belirlenmiş ve bu doğrultuda ETSI TS 102 023 Zaman Damgası Hizmet Sağlayıcıları için İlke Gereksinimleri Dokümanı yayınlanmıştır.

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 31. maddesine göre *"ESHS, zaman damgası ve hizmetlerini sağlamakla yükümlüdür. Nitelikli elektronik sertifika sahibi, bu hizmeti talep etmesi halinde alır."* Görüldüğü üzere, Yönetmeliğin bu maddesi zaman damgası hizmetlerini ESHS'ler için zorunlu hale getirmiş ve bütün ESHS'lerin hizmetleri sağlamanın yanı sıra zaman damgası uygulama esasları ve zaman damgası ilkeleri yayınlama zorunluluğu doğmuştur.

[76] ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, V1.2.1, Valbonna – France, 2003 s. 7

Yönetmeliğin 3. maddesine göre;

Zaman Damgası İlkeleri: Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgeyi,

Zaman Damgası Uygulama Esasları: Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi,

ifade eder.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 10. maddesinde ise, *"ESHS, zaman damgası ve hizmetlerine ilişkin olarak;*

a) CWA 14167-1 ve
b) ETSI TS 101 861
standartlarına uyar.

Zaman damgası ilkeleri ve zaman damgası uygulama esasları ETSI TS 102 023'e uygun olarak hazırlanır " şeklinde belirtilmiştir.

Ülkemizdeki uygulamada zaman damgası ilkeleri ve zaman damgası uygulama esasları hazırlanırken farklı çerçeveler ortay konulmaktadır. Kimi ESHS'ler zaman damgası uygulama esaslarını ve ilkelerini RFC 3647 6.8 başlığı altında sertifika ilkeleri ve sertifika uygulama esaslarının içerisinde yayınlamış, kimi ESHS'ler ise RFC 3647 çerçevesi doğrultusunda bu dokümanı hazırlamıştır. Kanaatimizce zaman damgası uygulama esasları ve ilkeleri hazırlanırken Yönetmelik'te belirtilen ETSI TS 101 023 standardının içerik çerçevesi baz alınmalıdır.

D. GÜVENLİ ELEKTRONİK İMZA OLUŞTURMA UYGULAMASI VE DOĞRULAMA ARAÇLARI İÇİN YAPILMASI GEREKEN BİLDİRİMLER

I. Güvenli Elektronik İmza Doğrulama Araçları

5070 sayılı Elektronik İmza Kanunu'nda, **"**Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"te ve "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de "güvenli elektronik imza doğrulama araçları"nın kullanımına ilişkin hukuki sonuçlar ve bu araçların isterlerine ilişkin hükümler bulunmaktadır.

Elektronik İmza Kanunu'nun 7. maddesine göre güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

İmza doğrulama araçlarıdır.

"Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"in 16. maddesine göre üçüncü kişiler "Nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla" yükümlüdürler. Yönetmelik'te belirtilen üçüncü kişiler nitelikli elektronik

sertifika kullanılarak yaratılan bir güvenli elektronik imzalı veriyi alan ve bu veriye güvenerek işlem yapan kişilerdir. Yönetmeliğin 16. maddesinden anlaşıldığı üzere üçüncü kişilerin yükümlülüklerini yerine getirmeleri için ya maddede belirtilen kontrolleri gerçekleştirmeleri ya da "güvenli elektronik imza doğrulama araçları"nı kullanmaları gerekmektedir. Uygulamada üçüncü kişinin bu kontrolleri yerine getirdiğini kanıtlaması neredeyse imkânsız olacağı için hem bu yükümlülüğün yerine getirildiğinin kanıtlanması hem de kullanım kolaylığı açısından "elektronik imza doğrulama araçları" elektronik imza uygulamasında özellikle son kullanıcılar ve kendi uygulamalarında elektronik imzalı veriler kabul eden kurumlar açısından olmazsa olmaz bir araç haline gelecektir[77].

"Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 8. maddesine göre "Elektronik sertifika hizmet sağlayıcı (ESHS), sağlamış olduğu güvenli elektronik imza doğrulama araçları için CWA 14171 standardına uyar ve bunu yazılı olarak taahhüt eder." Tebliğ'de belirtildiği üzere "güvenli elektronik imza doğrulama araçları" CWA 14171 standardına uygun olmak zorundadır ve ESHS'ler kendi nitelikli sertifikalarıyla birlikte sağlamış oldukları güvenli elektronik imza doğrulama araçları için yazılı olarak CWA 14171 standardına uygunluk bildiriminde bulunacaklardır.

Bilindiği üzere "güvenli elektronik imza doğrulama araçları" yazılım üreticileri tarafından geliştirilen yazılımlardır. Tebliğ'de belirtilen standarda uygunluk yazılım firmaları tarafından yazılımın standardında belirtilen isterleri karşılaması yoluyla sağlanacaktır. CWA 14171 ve bu standarda ilişkin denetim süreçlerinin belirlendiği CWA 14172-4 standartları incelendiğinde güvenli elektronik imza doğrulama araçlarının standarda uygunluğunun "self-declaration" yöntemiyle kanıtlandığı görülmektedir[78]. Buna göre güvenli elektronik imza doğrulama aracı sağlayıcısı (yazılım

---

[77] International Contract Adviser, "Certification" and Signature Authentication in E-Commerce, Electronic Communication Law Review 6 (3); 2000, Kluwer Academic Publishers, S. 3-18.

[78] CEN Workshop Agreement, CWA 14172-4 EESSI Conformity Assessment Guidance - Part 4: Signaturecreation applications and general guidelines for electronic signature verification, March 2004 s. 6-8

geliştirici firma) CWA 14171 standardına uygun bir araç ürettiğini kamuoyuna duyurmakta ve aracın bu standarda uygun olduğunu taahhüt etmektedir. "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 8. maddesine göre ise araç sağlayıcısı tarafından yapılan "self-declaration"a ek olarak ESHS'lerin de söz konusu aracın CWA 14171 standardına uygun olduğunu yazılı olarak taahhüt etmeleri gerekmektedir. Telekomünikasyon Kurumu'nun maddedeki hükmü bu şekilde düzenlemesindeki amacı tüketicilere ek bir güvence sağlamak amacıyla yazılım sağlayıcının yanı sıra ESHS'nin de sorumluluk altına girmesini sağlamak ve söz konusu araç ile ESHS'nin sisteminin çalışabilirliğinin test edilmesini zorunlu hale getirmektir; zira "güvenli elektronik imza doğrulama araçlarının ESHS'nin nitelikli sertifikalarıyla çalışabilmesini sağlamak için her iki tarafta da gerekli bazı hukuki ve teknik gereksinimlerin sağlanması gerekmektedir[79].

Burada dikkat edilmesi gereken en önemli nokta yazılım üretici tarafından yapılacak "self-declaration" metninde "sınırlamalar"ın gösterilmesi durumudur. CWA 14171 standardı yapısal olarak bir kılavuz şeklinde hazırlanmıştır; buna göre standarda uygun olarak üretilmiş bir yazılımın her açıdan standardı desteklemesi gerekmemektedir. CWA 14171 standardı bir güvenli elektronik imza doğrulama aracı için gerekli olabilecek nitelikleri belirtmiş ve bu niteliklere uyumu ihtiyari olarak öngörmüştür; ancak uygulamada CWA 14171 uyumlu doğrulama araçlarının standartta belirtilen nitelikleri destekleyip desteklemediğinin son kullanıcılar tarafından anlaşılabilmesi için CWA 14172-4 standardı ile desteklenmeyen niteliklerin self declaration metninde bulunması zorunluluğu getirilmiştir. Bu noktada güvenli elektronik imza doğrulama aracı kullanacak kurumsal ve bireysel kullanıcıların self-declaration metninde yer alan sınırlamalara dikkat etmesi gerekmektedir, zira hem yazılım üretici hem de ESHS güvenli elektronik imza doğrulama aracı ile ilgili olarak sadece sınırlamalar içerisinde saymadıkları nitelikleri taahhüt etmiş bulunmaktadırlar.

---

[79] Braley, Sarah Wood, Why Electronic Signature Can Increase Electronic Transaction and The Need For Laws Governing Electronic Signatures, NAFTA; Law and Business Review of Americas 7 (3); Summer 2001, Kluwer Academic Publishers, S. 417 – 444.

Güvenli elektronik imza doğrulama araçlarının, elektronik imza kullanımıyla ilgili çok önemli bir işlevi daha bulunmaktadır. Yukarıda bahsedildiği gibi nitelikli elektronik sertifika kullanılarak yaratılan bir güvenli elektronik imzalı veriyi alan ve bu veriye güvenerek işlem yapan üçüncü kişiler, nitelikli elektronik sertifikanın geçerlilik kontrolünü yapmakla ve imzaya ilişkin doğrulama süreçlerini gerçekleştirmekle yükümlüdürler[80]. Üçüncü kişiler yine yukarıda belirtildiği güvenli elektronik imza doğrulama aracı kullanarak bu yükümlülüklerini yerine getirebileceklerdir. Üçüncü kişiler güvenli elektronik imza doğrulama aracı kullanmadıkları takdirde, söz konusu geçerlilik kontrollerini ve doğrulama süreçlerini, sertifika iptal listesi (CRL) veya çevrimiçi sertifika durum protokolü (OCSP) servislerini kullanarak gerçekleştireceklerdir. Ancak söz konusu servisler belirli bir zaman aralığını desteklemeleri sebebiyle bu durum uygulamada büyük problemlere yol açabilecektir; şöyle ki nitelikli elektronik sertifikalar sadece geçerlilik süreleri boyunca "CRL" ve "OCSP" dizinlerinde tutulduklarından dolayı nitelikli sertifikanın geçerlilik süresi sona erdikten sonra yapılan geçerlilik kontrolleri ve doğrulama süreçleri başarısızlıkla sonuçlanacak, imza geçersiz sayılacaktır. Bu örnekte elektronik imza sertifikanın geçerlilik süresi içerisinde atılmıştır ancak ilk doğrulama veya ilk doğrulamadan sonraki kontrol veya işlem amaçlı doğrulamalar geçerlilik süresinin tamamlanmasından sonra yapılmaktadır. Bu durum bankacılık, muhasebe, sigorta gibi uzun dönemli verilerin saklanmasını ve periyodik olarak denetlenmesini gerektiren uygulamalarda ciddi problemlere yol açabilecektir[81]. Ancak CWA 14171 standardı doğrultusunda zaman damgası ve uzun dönemli doğrulama niteliklerini destekleyen bir güvenli elektronik imza doğrulama aracı sayesinde bu sorun ortadan kaldırılabilmektedir.

---

[80] Jawahitha, Sarabdeen, Electronic Contract in Malaysian Contracts Act: 1950; An Analytical Comparison with the EU Directive on E-Commerce and the U.S. Uniform Computer Information Transaction Act 1999, Business Law Review 24 (4); April 2003, Kluwer Academic Publishers, S. 91 – 106.

[81] Lopez – Tarrvelle, Aurelio, A European Community Regulatory Framework For Electronic Commerce, Common Market Law Review 38 (6); December 2001, Kluwer Academic Publishers, S. 1337 – 1384.

Sonuç olarak; Güvenli elektronik imza doğrulama araçları, nitelikli elektronik sertifikaların geçerlilik kontrollerinin ve imza doğrulama süreçlerinin gerçekleştirilmesinde bireysel ve kurumsal kullanıcılara kolay ve otomatik çözümler sağlaması sebebiyle elektronik imza kullanımına ve elektronik imza ile ilgili farkındalığın sağlanmasına oldukça faydalı olacak araçlardır. Elektronik imza doğrulama araçları zaman damgası ve uzun dönemli doğrulama fonksiyonları ile elektronik imzanın kullanımında uzun dönemde ortaya çıkacak bazı problemlere çözüm olabileceklerdir. Ayrıca elektronik imzada yetkili imza probleminin aşılabilmesi ancak güvenli elektronik imza doğrulama aracı ile çalışabilen bir "signature policy"nin oluşturulması ile mümkün olabilecektir. Söz konusu gereksinimlerin yerine getirilmesi için gerekli hukuki ve teknik analiz çalışmalarının tamamlanması ve bu doğrultuda ortaya konacak teknik çözümün hem uygulama sağlayıcı (kurumsal yapı) hem de son kullanıcılar tarafında yapılandırılması gerekmektedir.

II. Güvenli Elektronik İmza Oluşturma Uygulamaları

Güvenli elektronik imza oluşturma uygulamaları, güvenli elektronik imza sistemi içerisindeki, elektronik imzanın atılacağı işlemin yapıldığı, elektronik imzanın atıldığı, ön yüzde imzalayan tarafından kullanılan, arka yüzde ise güvenli elektronik imza doğrulama aracına, arşiv bölümüne ve varsa işlemin devam ettirileceği diğer bölümlere bağlanan uygulamadır[82].

Güvenli elektronik imza oluşturma uygulaması, güvenli elektronik imza sistemi içerisinde güvenlik gereksinimlerinin en önemli olduğu parçadır.[83] Zira güvenli

[82] Nödler J.M., Legal Framework of Electronic Signatures in the European Union and Germany, Seminar in Network Security Institute of Computer Science Georg-August-Universitat Gottingen, February 2006 Uniform Manufacturer Declarations for Signature Products, s. 18

[83] Scheuermann D., Schwiderski-Grosche S., Struif B., Usability of Biometrics in Relation to Electronic Signatures, GMD – German National Research Center for Information Technology Institute for Secure Telecooperation (SIT), September 2000 s.22

elektronik imza oluşturma uygulaması, tamamen uygulama sağlayıcının kontrolünde olduğu için imzalayanın ve varsa doğrulayan üçüncü kişinin, sistemin güvenliğinden emin olması gerekir[84]. Burada özellikle belirtmek gerekir ki, güvenli elektronik imza oluşturma uygulaması kesinlikle güvenli elektronik imza oluşturma aracı değildir. Güvenli elektronik imza oluşturma aracı, imza oluşturma ve doğrulama verilerinin yaratıldığı ve saklandığı, münhasır olarak sertifika sahibinin kontrolünde bulunan araçtır. Güvenli elektronik imza oluşturma uygulaması ise, güvenli elektronik imza aracı aracılığıyla kullanılabilen ve elektronik imzanın yaratılmasını tetikleyen uygulamadır. Burada güvenlik açığı riski elektronik imza üzerinde değil, imzalanacak veri üzerindedir. Yani, güvenlik kırılması sebebiyle, imzalayan, imzalamak istediği veriden başka bir veriyi imzalayabilir. Önyüzde imzalayana gösterilen veri ile arka yüzde imzalanan veri birbirinden farklı olabilir.

Güvenli elektronik imza oluşturma uygulamasının güvenlik açısından bu derece kritik olması sebebiyle Telekomünikasyon Kurulu 01.06.2006 tarihli Kararı ile güvenli elektronik imza oluşturma uygulamalarına ilişkin gereksinimleri belirlemiştir. Kurul kararında,

"Güvenli elektronik imza ile imzalanacak dokümanın görüntülenmesi için sağlamış olduğu imza oluşturma uygulamaları ve imzalanacak verilerin içerikleri ile ilgili olarak CWA 14170 (Security Requirements for Signature Creation Applications) "Elektronik İmza Oluşturma Uygulamaları için Güvenlik İhtiyaçları" standardına uyum sağlar ve bunu yazılı olarak taahhüt eder,

CWA 14170'e uyumlu olarak belirlediği imzalanacak dokümanların veri formatları konusunda kullanıcıları bilgilendirir.

Güvenli elektronik imzaların ETSI TS 101 733 veya ETSI TS 101 903 standardına uygun olarak oluşturulması tavsiye edilir."

[84] Sveda P., Matyas Jr.V., Digital Signatures and Electronic Documents: A Cautionary Tale Revisited, UPGRADE Vol. V, No. 3, June 2004 s. 40

şeklinde bir hüküm bulunmaktadır. Burada güvenli elektronik imza oluşturma uygulamaları için belirlenen sistem, bir önceki bölümde detaylı bir şekilde anlatılan güvenli elektronik imza doğrulama araçları ile aynıdır.

Kurul kararında dikkat edilmesi gereken bir diğer nokta, ESHS'nin CWA 14170'e uygun olarak belirlediği dokümanların veri formatları konusunda kullanıcıları bilgilendirmesi gerekliliğidir. Bilindiği üzere bazı veri formatları, içerdikleri değişkenler sebebiyle, veri okuyucuları tarafından farklı yorumlanabilmekte ve farklı sonuçlar doğurabilmektedirler. Örnek vermek gerekirse, imzalayan bir başvuru formunu doldururken, ücret ile ilgili kısma 100 YTL girip bu formu imzaladığında;eğer form farklı veri okuyucular (farklı veri okuyucu veya aynı okuyucunun farklı versiyonu) tarafından okunabiliyorsa 100 YTL'lik kısım değişkenler sebebiyle 100 $ veya 1000 YTL gibi farklı sonuçlar gösterebilir. Böyle bir dokümanda, imza doğrulaması yapıldığında imza geçerli sonucunu verecektir, zira imzalanan veride bir değişikli olmamıştır. Ancak veri farklı okuyucular tarafından farklı yorumlanmaktadır. Bu sorunun aşılması için Kurum bünyesinde yapılan çalışmalarda, statik veri formatlarının ortaya konulması ve imzalama işlemlerinin sadece bunlarla yapılması fikri ortaya atılmıştır. Kurum da yukarıda belirtilen kararıyla bu sorumluluğu ESHS'lere bırakmış gözükmektedir. Kanaatimizce bu karar oldukça yanlıştır. Öncelikle imzalanabilecek veri formatlarının ESHS'ler tarafından belirlenmesi açık bir şekilde rekabet ihlali doğurabilecek bir durumdur. Çünkü söz konusu veri formatlarının çoğu özel şirketler tarafından geliştirilen ürünlerin çıktılarıdır. Böyle bir durumda ESHS'lerin hangi objektif kriterlerle imzalanabilecek veri formatlarını belirleyeceği sorusunun cevabı bulunmamaktadır. Ayrıca imzalanabilecek veri formatlarının belirlenmesi oldukça uzun ve pahalı değerlendirme aşamalarına ihtiyaç duymaktadır ve mevcut ESHS'lerin hiçbirisi bu değerlendirmeyi yapabilecek kapasitede değildir. Eğer bir veri formatı seçimi yapılacaksa bu regülatör Kurum olan Telekomünikasyon Kurumu tarafından yapılmalıdır.

Veri formatlarıyla ilgili bu problemin çözümü için kanaatimizce en mantıklı yol, imzalanan verinin formatına ilişkin bilginin, ETSI TS 101 733 standardı ile

belirlenen imzalanan nitelikler içerisinde bulunmasıdır. ETSI TS 101 733, madde 5.2 de belirtilen "data content type" ile imzalanan verinin formatı imzalı özellikler içerisine girilirse, imza doğrulama aracı, bu bilgi ile veriyi doğru okuyucu ile açabilecektir. Bu sorunun çözümü için önerilebilecek bir başka yol ise imza ilkeleri dokümanın içerisinde ilgili imza uygulamasında kullanılan veri formatının belirtilmesi ve bu imza ilkesine imza içerisinde referans verilmesidir. ETSI TS 101 7332'de belirlenen, "explicit policy electronic sigantures" formatına dahil elektronik imzalarda imza ilkeleri referansı imza verisi içerisinde yer almaktadır. Kurul kararıyla da, yaratılacak elektronik imzaların ETSI TS 101 733 veya bu formatın XML versiyonu olan ETSI TS 101 903'e uygun olarak yaratılması tavsiye edilmiştir.

E. ELEKTRONİK İMZADA YETKİ VE İMZA İLKELERİ (SIGNATURE POLICIES)

Elektronik İmza Kanunu'na göre güvenli elektronik imza oluşturmak için kullanılan nitelikli elektronik sertifikalar sadece gerçek kişilere sağlanabilmektedir; şirketler, kamu kurumları, dernek ve vakıflar gibi tüzel kişiler nitelikli elektronik sertifika sahibi olamayacaklardır. Bu durumda tüzel kişiliğin elektronik ortamda hukuki bir işlem yapabilmesi için tüzel kişiliği temsil ve ilzam yetkisine sahip gerçek kişilerin güvenli elektronik imzalarına ihtiyaç duyulacaktır. Söz konusu kurum ve kuruluşların yetkili temsilcileri vasıtası ile gündelik hayatın akış ve süratine uygun olarak işlem yapabilmesi imza sirküleri ile mümkün olmaktadır. Ancak elektronik ortamda tüzel kişilik adına imza yetkisine sahip kimselerin bu yetkilerinin sadece güvenli elektronik imza ile doğrulanması mümkün değildir. Elektronik İmza Kanunu'nun 9. maddesinin (g) bendine göre *"sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin"*, (h) bendine göre ise *"Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin"* nitelikli elektronik sertifikada yer alması zorunludur. Söz konusu 9. Maddeden anlaşıldığı üzere bir imza sirkülerinde veya herhangi bir yetki belgesinde tanımlanan yetki ile ilgili bilgiler, elektronik sertifikaların teknik özellikleri de göz

önüne alınarak düşünüldüğünde nitelikli elektronik sertifikada ya doğrudan metin halinde ya da bir tanımlayıcı aracılığıyla yer alması gerekmektedir. Meseleyi hukuki açıdan ele aldığımızda ise söz konusu kurum ve kuruluşların yetkili organları vasıtası ile temsilcilerine devredebilecekleri yetkilerin çeşitliliği ve bu yetkilerin kısa bir metinle düzenlenmenin zorluğu dikkate alındığında ifade edilen yetkilerin metin haliyle bir elektronik sertifikaya girilmesinin mümkün olmayacağı aşikardır. Ayrıca değişen ihtiyaçlar karşısında yetkilerin dinamik yapısı ve yetki tanım ve onay işleminin elektronik sertifika hizmet sağlayıcıların hak ve sorumlulukları kapsamı içerisinde yer almaması nedenlerine bağlı olarak, yetki ile ilgili bilgilerin sertifikada statik olarak belirtilmesi sorunlara yol açabilecektir.

Yetki bilgilerinin dinamik olarak elektronik imzada gösterilebilmesi için söz konusu elektronik imza uygulaması doğrultusunda dinamik yetki şemalarının hazırlanması ve yetki şemalarıyla ilgili statik yetki tanımlayıcılarının belirlenmesi gerekmektedir. Uygulamada birbirleriyle çalışabilir bu iki eleman, hukuki ve teknik altyapısı bulunan "signature policy" belgeleriyle somut hale getirilmektedir[85]. Ancak "signature policy" planlanan elektronik imza uygulaması kapsamında tasarlanıp, dikkatli bir belge, imza yetkilisi ve iş süreçleri analizinin tamamlanmasından sonra hazırlanmalıdır[86]. Yetki tanımlaması imza doğrulama süreçlerinde önem kazandığı için uygulamada signature policy belgeleri "güvenli elektronik imza doğrulama araçları" tarafından işleme tabi tutulacaktır; burada dikkat edilmesi gereken nokta güvenli elektronik imza doğrulama aracının signature policy belgelerini okuyabilir ve otomatik süreçler dahilinde işleyebilir niteliklere sahip olması gerektiğidir[87].

[85] ETSI TR102 045, Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model, V1.1.1, Valbonna – France, 2003 s. 13

[86] Scheibelhofer K., Signing XML Documents and the Concept of "What You See Is What You Sign", Institute for Applied Information Processing and Communications at Graz University of Technology, January 2001 s. 21

[87] ETSI TR 102 041, Signature Policies Report, V1.1.1, Valbonna – France, 2002 s. 18

SONUÇ

Elektronik imza uygulaması, çeşitli topluluk uygulamalarının geliştirilmesiyle kısa dönemde günlük ticari ve idari hayatımızda gerektiği yeri elde edecektir. Elektronik imza uygulaması mevcut elektronik imza düzenlemeleriyle ciddi bir düzenleme çerçevesine kavuşmuştur. Gerek ikincil mevzuat gerekse de Telekomünikasyon Kurulu Kararıyla belirlenen uluslararası standartlar, elektronik imza uygulamasında ilgili taraflara çeşitli yükümlülükler ve sorumluluklar getirmekte, uygulamanın hayata geçirilebilmesi için söz konusu düzenlemelerde ve standartlarda belirtilen gereksinimlerin yerine getirilmesi gerekmektedir.

Elektronik imza uygulaması gereksinimlerinin en önemlilerinden birisi de dokümantasyondur. Elektronik imza uygulaması hem teknik hem hukuk hem de organizasyonel açıdan oldukça kapsamlı ve detaylı olması; bilgi güvenliği gerekçeleriyle tüm bu detaylara ilişkin gereksinimlerin bulunması sebebiyle tüm çerçevenin dokümante edilmesi gerekmektedir. ESHS tarafından ortaya konulan bu çerçeve; sertifika sahibi, kurumsal başvuru sahibi, diğer ESHS'ler gibi ilgili taraflarla yapılan karşılıklı sözleşmelerle ve sertifika ilkeleri, sertifika uygulama esasları ve imza ilkeleri gibi dokümanlarla ortaya konulmaktadır. ESHS tarafından ilgili taraflarla yapılan sözleşmeler, sözleşme serbestisi içerisinde değerlendirilecek olsa dahi elektronik imza ile ilgili mevzuat ve özellikle tüketici mevzuatına tabi olacaktır. Bu sebepten ötürü, sözleşmeler hazırlanırken, mevzuat doğrultusunda sözleşmelerde bulunması gereken hükümler ve sözleşmenin fiziki formatına ilişkin gereksinimler göz önünde bulundurulmalıdır. Sertifika ilkeleri ve sertifika uygulama esasları dokümanları oluşturulurken karşılıklı işlerliğin sağlanabilmesi amacıyla uluslararası standartlara uyum gösterilmesine dikkat edilmelidir. Özelikle sertifika ilkeleri dokümanlarının, katılımcılardan herhangi biri tarafından yaratılabileceği unutulmamalı ve çapraz uygulamalar içerisinde ilkelerin bağdaşması "polciy-mapping" yöntemi kullanılarak sağlanmalıdır.

Ülkemizdeki elektronik imza altyapısı ile ilgili en büyük eksiklik akreditasyon yapısının kurulmamış olmasıdır. Bu yapının bulunmamamsı sebebiyle özellikle elektronik imza uygulamaları ve elektronik imza doğrulama araçlarıyla ilgili standardizasyon uyumu denetimi yapılamamaktadır. Uygulamada fiili akreditasyon, ilgili mevzuat ve Telekomünikasyon Kurumu kararlarıyla ESHS'ler tarafından yapılmakla beraber bu durum hem elektronik imza ürünleri piyasasında eşitsizliklere yol açabilecek hem de uygulama geliştirmeleri doğrultusunda güncellenmiş somut gereksinimlerin ortaya çıkarılmasını engelleyecektir.

Elektronik imza uygulamasında karşılaşılacak ciddi sorunlardan bir tanesi de yetki bilgilerinin elektronik imza aracılığıyla belirtilememesidir. Kağıt ortamında bu sorun, imza sirküleri ile çözülürken benzer bir çözümün elektronik ortamda elektronik imza uygulamaları için de geliştirilmesi gerekmektedir. Bu sorunun çözümü için mevcut teknolojiler doğrultusunda en uygun çözümlerden birisi imza ilkeleridir; ancak ülkemizde konuyla ilgili yeterli teknik çalışma yapılmamıştır. İmza ilkeleri konusunda yapılacak çalışmalar ile imza ilkeleri şablonları belirlenmeli, referans imza ilkeleri yayınlanmalı ve imza ilkeleri ile çalışan imza oluşturma uygulamaları ve imza doğrulama araçları geliştirilmelidir. Söz konusu çalışmaların yapılması ile uzun süredir beklenen elektronik imza yaygınlığına kavuşulacak ve ülkede günümüze kadar konuyla ilgili yapılan yatırımların geri dönüşü sağlanabilecektir.

KAYNAKÇA

CEN Workshop Agreement, CWA 14171 General guidelines for electronic signature verification, May 2004

CEN Workshop Agreement, CWA 14170 Security requirements for signature creation applications, May 2004

CEN Workshop Agreement**,** CWA 14172-4 EESSI Conformity Assessment Guidance - Part 4: Signaturecreation applications and general guidelines for electronic signature verification, March 2004

CEN Workshop Agreement**,** CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, June 2003

CERN Certification Authority, Certificate Policy and Certification Practice Statement, Draft Version 1.1, April 2003

Certification Practice Statement and Subscription Agreement ("CPS") For Wireless Application Protocol (WAP) Server Test Certificates, Version 1.0, November 2000

Certipost E-Trust Services, Certification Practice Statement for Qualified and Normalised Certificates, Version 1.0, December 2003

CNRS/CNRS-Projets/Datagrid-fr, Certificate Policy and Certification Practice Statement, Version 0.3, August 2002

Collins. T. DESS Droit de l'Internet - Administration – Entreprises, Aspects techniques et juridiques des infrastructures de gestion de clés publiques, septembre 2004

Comodo Group, Comodo Certification Practice Statement, April 2003

Déler-Castro G., Cruellas-Ibarz J., Electronic Signature Functionality and Security Requirements, UPGRADE Vol. V, No. 3, June 2004

Dexia Root CA Certification Practice Statement, Version 1.0, April 2002

Dumortier J., Kelm S., Nilsson H., Skouma G., Eecke P.V., The Legal and Market Aspects of Electronic Signatures, Interdisciplinary Centre For Law and Information Techonology, 1999

e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları, Kasım 2005

Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, İstanbul, Temmuz 2004

ESnet Root CA Certificate Policy And Certification Practice Statement, Version 1.0, January 2003

European Commission, Certıficate Practıce Statement, Version 1.0, February 2002

European Commission in the framework of the SPRITE-S² pilot action, Guidelines, Methodologies and Standards to set up a CA for Digital Signatures

ETSI TR 102 041, Signature Policies Report, V1.1.1, Valbonna – France, 2002

ETSI TR 102 045, Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model, V1.1.1, Valbonna – France, 2003

ETSI TS, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.1, Valbonna – France, 2006

ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), V1.6.3, Valbonna – France, 2005

ETSI TS101 862, Qualified Certificate profile, V1.3.3, Valbonna – France, 2006

ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, V1.2.1, Valbonna – France, 2003

ETSI TS102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, V1.2.2, Valbonna – France, 2005

Ferrer-Gomila J., Payeras-Capellà M., Certification Practise Statements: The National Mint of Spain's Experience, UPGRADE Vol. V, No. 3, June 2004

Forum of European Supervisory Authorities for Electronic Signatures (FESA), Working Paper on Qualified Certificates for Automatically Signing Systems, October 2004

Hindelang S., No Remedy for Disappointed Trust – The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared, Journal of Information, Law and Technology, March 2002

Identrus Identity Certificate Policy IP-ICP Version 2.0, 2003

Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, PKI Assesment Guidelines, American Bar Association publishing, June 2001

Information Security Committee Electronic Commerce and Information Technology Division, Digital Signature Guidelines, American Bar Association, August 1996

Kiran S., Lareau P., Lloyd S., PKI Basics - A Technical Perspective, PKI Forum, November 2002

Lloyd S., Fillingham D., CA-CA Interoperability, PKI Forum, March 2001

Menzel T., Schweighofer E., Liability of Certification Authorities: The present legal situation and the need for abstract liability of certification authorities, User Identification & Privacy Protection, Joint IFIP WG 8.5, WG 9.6, Working Conference 1999, Schweden K., DSV, S. 161-172

Network Working Group, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

Network Working Group, Internet X.509 RFC 3280 Certificate and Certificate Revocetion List Profile, April 2002

Nilsson H., Eecke P.V., Medina M., Pinkas D., Pope N., European Electronic Signature Standardization Initiative (EESSI), Final Report of the EESSI Expert Team, July 1999

Nödler J.M., Legal Framework of Electronic Signatures in the European Union and Germany, Seminar in Network Security Institute of Computer Science Georg-August-Universitat Gottingen, February 2006

Performance Engineering Corporation, Public Key Infrastructure Analysis, PEC Solutions, Inc.Virginia, March 2000

Politique de Certificat Relative Au Certificat Qualifie Ou Normalise Certipost E-Trust, Version 1.0, Mai 2004

Polk W.T., Hastings N.E., Bridge Certification Authorities: Connecting B2B Public Key Infrastructures, National Institute of Standards and Technology

Ribagorda-GarnachoA.,Electronic Signature at the Heart of Information Security Developpement: An Overview", UPGRADE Vol. V, No. 3, June 2004

Sabo J.T., Dzambasow Y.A., PKI Policy White Paper, PKI Forum, March 2001

Scheibelhofer K., Signing XML Documents and the Concept of "What You See Is What You Sign", Institute for Applied Information Processing and Communications at Graz University of Technology, January 2001

Scheuermann D., Schwiderski-Grosche S., Struif B., Usability of Biometrics in Relation to Electronic Signatures, GMD – German National Research Center for Information Technology Institute for Secure Telecooperation (SIT), September 2000

Sevim T., İstanbul Barosu Staj Eğitim Merkezi, Bireysel Çalışma Raporu, Elektronik İmzanın Hukuksal Boyutları: Mevcut Durum Eksiklikler ve Çözüm Önerileri, İstanbul, Şubat 2005

Smedinghoff T.J. , Certıficatıon Authorıty Lıabılıty Analysıs, Baker & McKenzie, Chicago

Soran S., Gülaçtı E., Teknik Rapor: Nitelikli Elektronik Sertifika Profili, TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), Ağustos 2005

Stapleton J., Biometrics, PKI Forum, May 2001

SUN Public Key Infrastructure Certification Practice Statement, Version 1.52, November 2000

Sveda P., Matyas Jr.V., Digital Signatures and Electronic Documents: A Cautionary Tale
Revisited, UPGRADE Vol. V, No. 3, June 2004

VeriSign Certification Practice Statement, Version 2.3 March 2004

VeriSign Trust Network European Directive Supplemental Policies, Version 1.0, September 19, 2001

VeriSign Trust Network Certificate Policies, Version 1.3, March 2004

Yıldız E., A Propsal For Turkish Government Public Key Infrastructure Trust Model, December 2001