TBD Kamu-BİB
Bilişim Platformu VII
26-29 Mayıs 2005
Antalya

e-imza
NİTELİKLİ SERTİFİKASYON ALTYAPISI VE YETKİLENDİRME

1. ÇALIŞMA GRUBU

Hazırlayanlar :

Muzaffer YILDIRIM
Altuğ YAVAŞ
Önder ÖZDEMİR
Adnan METE
Adnan COŞKUN SAKARYA
Recep SADIK
M. Kemal NALÇACI
Cemal GEMCİ
Zülfi GÜREN

İÇİNDEKİLER

EKLER :

EK-A : Elektronik İmza Kanunu

EK-B : Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

EK-C : Kamu Sertifikasyon Merkezi oluşturma Genelgesi

EK-D : Resmî Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik

EK-E :Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (Tebliğ)

EK -F : Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı(Tebliğ)

KAYNAKÇA

1 Özet

Ülkemizde dünyayla eş zamanlı olarak elektronik hayata geçiş çalışmaları sürdürülmektedir. Bu konu hem hükümet, hem de sistemi oluşturacak sektör (yazılım, donanım, akıllı kart gibi) tarafından büyük destek görmektedir. Günlük hayatımızda yaşadığımız birçok olayın, hizmetin elektronik ortama aktarılmasının sayısız faydalı sonuçlar doğuracağı açıktır. Elektronik ortamda yapılan uygulama ve hizmetler, kağıt ortamına oranla zaman, iş gücü, para tasarrufu sağlayacak, hizmetlerin 7 gün 24 saat alınıp verilebilmesine olanak sağlayacak, bütün dünyayı bir ağ ortamında birleştirebilecektir. Elektronik ortama geçiş farklı bir döneme geçişi sağlayacak, hizmet konusundaki anlayışı değiştirerek hizmetin vatandaşın ayağına gitmesine imkan tanıyacak, elektronik ticaret müşteri kitlesini sadece çevrenizdeki insanlar olmaktan çıkarıp dünyanın tümüne yaygınlaştırabilecektir. Ancak elektronik ortama geçiş birçok riski de beraberinde getirecektir. Ağ ortamında yapılan işlemlerden karşı tarafın kim olduğundan emin olmak güçleşecek, gönderilen bilgilerin bozulmadan/değiştirilmeden gitmesinden şüphe duyulacak, yapılan işlemlerin inkar edilme endişesi yaşanacaktır. Elektronik ortamda bu risklerden kurtulmak için kullanılacak araç elektronik imzadır.

Elektronik imza, gerçek hayatta ıslak imza ile yapılan her işin (kanunla hariç tutulanlar dışında: evlenme, tapu işlemleri gibi) elektronik ortamda yapılabilmesi için bir araçtır. Elektronik imza da tıpkı ıslak imzada olduğu gibi evrakla kişinin kimliği arasında bir ilişki oluşturur. Ancak elektronik imzanın ıslak imzaya oranla üstünlükleri de vardır. Islak imzaya oranla taklit edilmeleri imkansız denecek oranda zordur, ayrıca sadece kişinin kimlik bilgisiyle değil ayrıca mesajın içeriğiyle de ilişkilidir. Mesajdaki en küçük değişikliklerde bile elektronik imza değişir. Bu nedenle mesajın bütünlüğünü (bir yerden bir yere giderken bozulmadan, değiştirilmeden, orijinal haliyle gitmesi) sağlamada oldukça önemli bir rol oynar. Elektronik imza ıslak imza gibi görsel bir ifade değildir. Elektronik ortamdaki hemen hemen her uygulamada mesajın sonuna eklenen bir veridir. Elektronik imza sayesinde kimlik doğrulama, veri bütünlüğü ve inkar edememe özellikleri sağlanır. Ancak elektronik imza verinin gizliliğine ilişkin bir çözüm yaratmaz. Mesajların başkaları tarafından görülmemesi, başkalarından gizlenmesi isteniyorsa şifreleme tekniğinin kullanılması gereklidir. Elektronik uygulamalarda hem gizlilik hem de yukarıda sayılan üç özelliğin sağlanması için imzalama ve şifreleme teknikleri birlikte kullanılırlar.

Elektronik imza sadece bir altyapıdır. Elektronik uygulamalarda elektronik imzanın kullanılabilmesi için birçok uygulama ile entegrasyonu için ek yazılımlara ihtiyaç olacaktır. Örneğin kullanılmakta olan bir doküman yönetim sisteminde elektronik imza kullanımının sağlanması için yazılıma entegrasyon modüllerinin eklenmesi gerekecektir. Benzetme yapmak gerekirse elektronik imza doğalgaz olarak düşünülürse, doğalgazın kullanımı için ya doğal gaz uyumlu soba/ocak/kombi alınacaktır ya da kömürle çalışan araçlar doğalgazla çalışır hale getirilecektir. Kısacası elektronik imza kullanımına geçilmesi için öncelikle uygulamaların elektronik ortama aktarılması ve elektronik imza ile çalışabilir hale getirilmesi gerekecektir.

Elektronik imza hukuksal olarak ıslak imzaya eşdeğerdir. Bu anlamda Türkiye'de gerekli kanun, yönetmelik ve tebliğler hazırlanmıştır. İlgili yayımlanan mevzuatlarda konuyla ilgili gerekli açıklamalar yapılmıştır. Mevzuata göre sertifikaların hukuksal olarak geçerli olması için nitelikli olması gerekmektedir. Nitelikli sertifikalar da ancak Telekomünikasyon Kurumu'ndan lisans almış Elektronik Sertifika Hizmet Sağlayıcıları tarafından temin edilebilir. Ülkemizde henüz lisanslı

Elektronik Sertifika Hizmet Sağlayıcısı yoktur (henüz başvurular yapılıyor, kanuna göre başvurudan sonra minimum 2 ay onaylama süreci var). Ancak yılın ikinci yarısında bu sistemin yerleşeceği tahmin edilmektedir. Yayınlanan Başbakanlık genelgesi ile Türkiye'de kamu çalışanlarına ait sertifikalar için bir düzenleme getirilmiş (kamu çalışanları sertifikalarını TÜBİTAK'tan alacaklar), vatandaş sertifikaları konusu düzenlemeye açık bırakılmıştır. Vatandaş elektronik imza anahtarı ve sertifikasını nitelikli elektronik sertifika sağlayan özel kuruluşlardan alacaktır (aday kuruluşlar TÜRKTRUST ve E-GÜVEN). Vatandaş sertifikasını bu kuruluşların yönlendirdiği noktalardan (Kayıt Merkezleri : Banka şubeleri, noterler, üniversiteler, belediyeler olabilir) kişisel başvuru yaparak alabilir. İmzalama anahtarı ve sertifikalar yönetmelik tanımına göre akıllı kart ya da token (akıllı çubuk) denen araçlarda taşınacak ve her imzalama işleminde bu araçlar bilgisayar, kiosk ya da benzeri cihazlara takılacak. Akıllı kartların çalışması için ayrıca akıllı kart okuyuculara ihtiyaç var, tokenlar USB portundan direk bağlantı sağlayabiliyor. Ancak özellikle bankaların EMV standardına uyum nedeniyle akıllı kart verecek olmaları ve akıllı kartların işlevsel kolaylıkları nedeniyle eğilimin daha çok akıllı kart kullanımı yönünde olacağı tahmin edilmektedir. Vatandaş imzalama anahtarı ve sertifikasını alırken ya ücretini kendi ödeyecek ya da kampanyalardan yararlanacak. İmzalama anahtarı ve sertifikanın ömrü özel bir tanımlama olmazsa 1 (bir) yıl. Sertifikanın ömrü bittiğinde ücreti ödenerek yenilenecek.

Elektronik imza konusu oldukça yeni bir konudur ve dikkatli davranılmadığı durumda riskler taşıyabilir. Konu doğrudan güvenlikle ilgili olduğu için önemi oldukça yüksektir. Bu nedenle alınacak yazılım, donanım ve hizmetler konusunda çok dikkatli olunması, bilinçli yaklaşılması, yabancı ülke katkısının incelenmesi, güvenilirlik/süreklilik/kurumsallık sorgulamalarının iyi yapılması ve hizmet kalitesinin doğru değerlendirilmesi faydalı olacaktır.

Elektronik hizmetlerin hızla yaygınlaşmasının, hem bu hizmetleri veren hem de bu hizmetlerden faydalananlar açısından en çabuk akla gelen nedenleri şunlardır:

- Erişim tarifelerin ucuzlaması
- Erişim hızının artması
- Zaman, iş gücü, para tasarrufu
- Kullanım kolaylığı
- Elektronik olarak verilen hizmetin hukuki olarak geçerlilik kazanması.

Bunlar gibi sayılabilecek daha birçok nedenden dolayı tüm dünyada olduğu gibi ülkemizde de kamu kurumları, vatandaşa verdikleri hizmetleri ve kendi kurumsal iş akışlarını elektronik ortama taşımak için kapsamlı projeler başlattılar. Maliye Bakanlığı'nın "Vergi Dairesi Otomasyon Projesi", Adalet Bakanlığı'nın "Ulusal Yargı Ağı Projesi", Sağlık Bakanlığı'nın "Aile Hekimliği Bilgi Sistemi", günlük hayatta toplumu en çok etkileyen ve etkileyecek olan projelere örnek olarak verilebilir.

Mevcut e-Devlet projelerinden sağlanan verimin artarak devam ettirilmesi ve yeni projelerin hayata geçmesi aşamasında, kurumların karşı karşıya olduğu en önemli risklerden biri iletilen bilginin güvenliğinin sağlanmasıdır. "**Elektronik imza**", değerli ve kişiye/kuruma özel bilgilerin İnternet gibi açık ve korumasız ağlar üzerinden güvenli olarak iletilmesinde kullanılan bir teknolojidir. Elektronik İmza teknolojisi ve Elektronik İmza teknolojisi kullanılarak oluşturulan Açık Anahtar Altyapısı Bölüm 2'de açıklanmıştır.

Ülkemizde elektronik imza teknolojisinin etkin kullanımına yönelik olarak gerçekleştirilen çabalar 15 Ocak 2004'de 5070 nolu **Elektronik İmza Kanunu**'nun ve bu kanunla ilişkili yönetmelik ve tebliğin yayınlanması ile sonuç verdi. Bu kanunla "Elektronik İmza" teknolojisinin ülkemizdeki kamu ve özel sektör uygulamalarında nasıl hayata geçirileceği ile ilgili hukuki bir altyapı oluşturulmuş oldu. Bu yasa ile tanımlanan güvenli elektronik imza, ıslak imza ile aynı hukuki sonuçları doğurmaktadır (Madde 5).

Elektronik imza teknolojisinin en önemli parçası, kurum ve kişiler arasında bir güven köprüsü kurulmasını sağlayan **Elektronik Sertifika Hizmet Sağlayıcılar (ESHS)**'dır. Bölüm 0'de oluşturulan yasal altyapı ile ESHS'lere yüklenen görevler belirtilmiştir. Daha sonra Bölüm 4'de bir ESHS'nin bu görevleri yerine getirebilmek için sahip olması gereken nitelikler tarif edilmiştir. Ayrıca herhangi bir elektronik imza ve yasal hükme sahip "güvenli elektronik imza" arasındaki farklar açıklanmıştır.

Bölüm 5'de Türkiye'deki kamu ve özel sektörde ESHS yapılanması, Kamu Sertifikasyon Yapısı'nın oluşturulması ile ilgili bilgiler verilmiştir.

Elektronik imzanın temel işlevi uygulamalar için güvenli bir iletişim ortamının kurulmasıdır. Elektronik imzanın, uygulamalardan farkı ve birlikte çalışabileceği uygulamalar Bölüm 6'da gerçek örnekler de verilerek açıklanmıştır.

Elektronik imza, Avrupa Birliği, Amerika Birleşik Devletleri ve diğer ülkelerde de yasal altyapısı oluşturulmuş olan ve devlet ve özel sektörde kullanılmakta olan bir teknolojidir. Bu yönden yurtdışındaki uygulamalarla birlikte çalışabilirliğin sağlanması gereken noktalarda yapılması gerekenlerle ilgili bilgiler Bölüm 7'de verilmiştir.

Elektronik imzaların istenen düzeyde bir güven altyapısı sağlayabilmesi için önemli bir halka, bu teknolojinin matematiksel altyapısını içinde barındıran akıllı kart ve akıllı çubuk gibi kriptografik araçlardır. Bölüm 6'de bu araçlar hakkında bilgiler verilmiş ve günlük hayatta kullanımları ile ilgili karşılaşılabilecek hususlar ele alınmıştır.

2 Güvenli Veri İletimi ve Elektronik İmza

2.1 Temel Gereksinimler

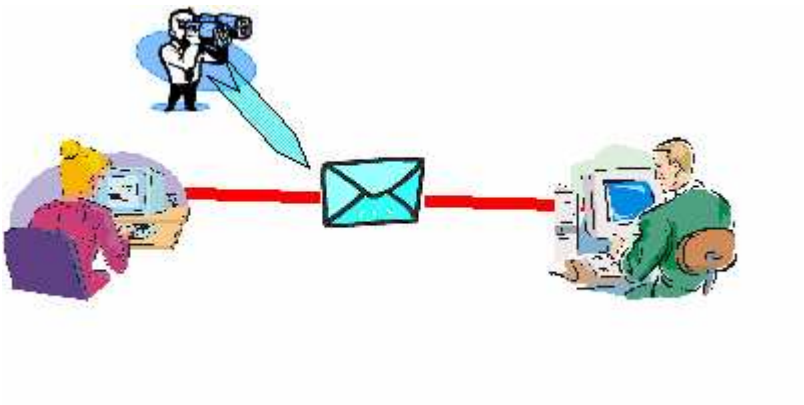
Elektronik İmza Yasası'nda Elektronik imza şöyle tanımlanmaktadır:

"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri." (Yasa Madde 3b)

Elektronik imza, iletişim ve veri güvenliğini sağlamak amacıyla geliştirilmiş bir teknolojidir. Günümüzde İnternet başta olmak üzere açık ve korunmasız ağlar üzerinden gerçekleşen veri iletişiminin güvenliğinin sağlanması için bir takım gereksinimler belirlenmiştir. Elektronik işlemlerdeki temel güvenlik gereksinimleri şunlardır:

1. Gizlilik: Verinin/içeriğin görüntülenmesinin sadece veriyi görüntülemeye izin verilen şahısların erişimiyle kısıtlanmasıdır (Bkz. **Error!**

Reference source not found.). Bu şekilde, artık çok da zor olmayan ve kişisel bilgi mahremiyetini tehdit eden iletişim trafiğinin yetkisiz olarak dinlenmesine karşı bir önlem alınmış olur. Gizlilik bilginin şifrelenmesi ile gerçekleştirilebilir.



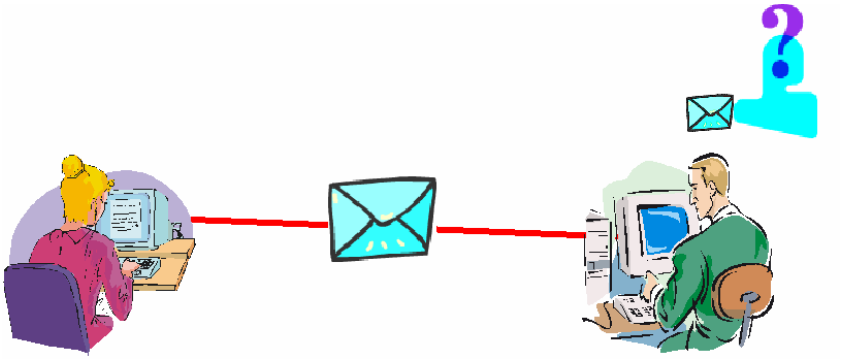
Şekil 1 Gizlilik

2. Bütünlük: Verinin izinsiz olarak veya yanlışlıkla değiştirilmesinin, silinmesinin veya veriye ekleme yapılmasının önlenmesidir (Bkz. **Error! Reference source not found.**). Bu şekilde verinin göndericiden alıcıya, göndericiden çıktığı haliyle değişmeden ulaşması sağlanır. Alıcı, iletinin göndericiden çıktığı haliyle kendisine ulaştığını bir bütünlük sınaması yapar anlar. Bütünlük gereksinimi, elektronik imza ile gerçekleştirilebilir.

Şekil 2 Bütünlük

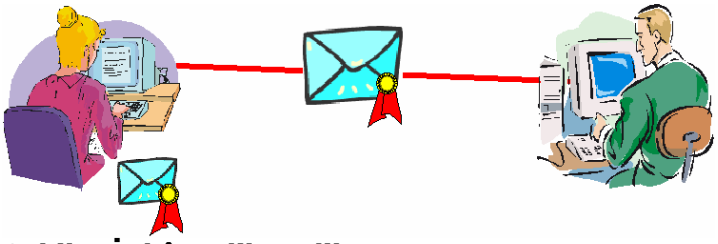
3. **Kimlik doğrulama:** Mesajın iletiminin geçerliliğinin ve mesaj sahibinin kimliğinin doğrulanmasının sağlanmasıdır. Örneğin bir elektronik posta mesajı üzerinde yer alan gönderici adresi, mesajın asıl göndericisi olmayabilir (

4. Şekil 3). Bu nedenle alıcı, göndericinin kimliğini doğrulamak için bir takım yöntemler kullanır. Elektronik imza, kimlik doğrulama için kullanılabilecek yöntemlerden biridir.



Şekil 3 Kimlik Doğrulama

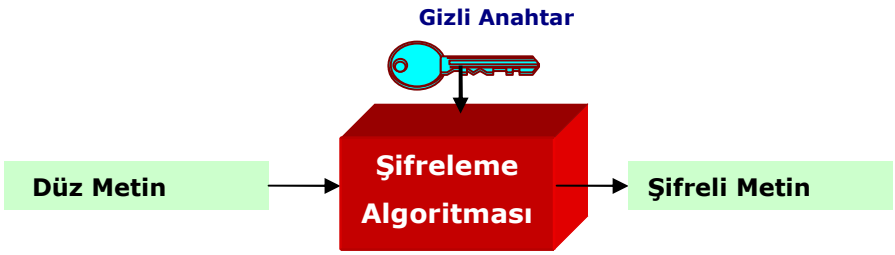
5. İnkâr Edilmezlik: Bireyerin elektronik ortamda gerçekleştirdikleri işlemleri inkar etmelerinin önlenmesidir (Şekil 4).



Şekil 4 İnkâr Edilmezlik

Yukarıdaki 1. gereksinimde de bahsedildiği gibi gizliliğin sağlanması bilginin şifrelenmesi ile gerçekleştirilebilir. Şifrelemede en yaygın kullanılan yöntem "*gizli anahtarlı şifreleme*" denen yöntemdir. Bu yöntemde mesaj şifrelenirken bir "anahtar" kullanılır ve şifrenin açılması için şifrelemede kullanılan anahtara ihtiyaç vardır (Şekil 5). Bu şifreleme yönteminin güvenliği anahtarın gizli tutulmasına bağlıdır. Anahtar "0" ve "1"lerden oluşan bir bit dizisidir ve her şifreleme algoritmasında farklı boylarda anahtarlar kullanılır. Örneğin gizli anahtarlı şifreleme algoritmasına örnek olarak verilebilecek AES algoritmasında 128 bit anahtar kullanılır. Anahtarlar, üretilirken rastgele sayı üreteci denen fonksiyonlardan yararlanılır.

Ancak yüzyıllar boyu kullanılan ve bir çok mesajı yabancılardan ve düşmanlardan korumaya yarayan gizli anahtarlı şifrelemenin de kendine özgü sorunları bulunmaktadır. Mesajın değiştirilmesinin önlenmesi, şifrelemede ve şifre çözmede kullanılan anahtarın gönderici ve alıcı arasında paylaşımı, mesajı gönderenin kimlik doğrulamasının yapılamaması çözülmesi gereken sorunlardır.



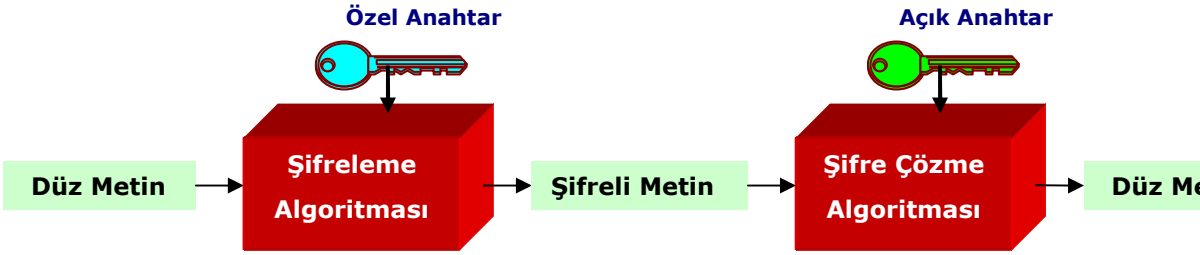
Şekil 5 Gizli Anahtarlı Şifreleme

Gizli anahtarlı şifrelemenin bu gibi sorunlarını aşmak için açık anahtarlı şifreleme yöntemleri geliştirilmiştir. Burada biri **açık** diğeri **özel** olarak nitelenen bir anahtar çiftinin bulunduğu (asimetrik) bir yöntem kullanılmaktadır. Bu iki anahtar, üretilirken

birlikte üretilirler. Yani matematiksel olarak aralarında gizli bir bağ bulunur. Bu sayede bir anahtar çiftindeki bir anahtar ile, diğer anahtarla şifrelenmiş bir metnin şifresi çözülebilir (

Şekil 6). Bununla birlikte bir anahtara sahip olan bir kişinin, matematiksel yollarla diğer anahtarı elde etmesi mümkün değildir. Şekil 7'de örnek olarak bir açık anahtar verilmiştir.

Açık anahtarlı şifreleme elektronik imza teknolojisinin temelini oluşturur. Bölüm 2.2'de açık anahtarlı şifreleme kullanılarak nasıl bir elektronik imza oluşturulduğu açıklanmıştır.



Şekil 6 Açık Anahtarlı Şifreleme

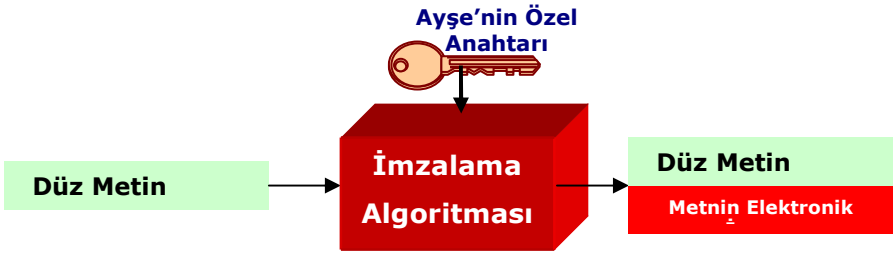
MIIF4jCCBMqgAwIBAgIKQg6ypAAAAAAAJjANBgkqhkiG9w0BAQUFADCBsDELMAkGA1UEBhMCVVMxCzAJBgN
VTRVJUcnVzdCBDbGllbnQgQXV0aGVudGljYXRpb24gYW5kIEVtYWlsMB4XDTAwMDQyNzE3NDQyM1oXDTAxMDQyNz
CBUaXRsZSBDbzElMCMGA1UECxMcaHR0cDovL3d3dy51c2VydHJ1c3QuY29tL2NwczEaMBgGA1UEAxMRTWFydGluIF

Şekil 7 Açık Anahtar

2.2 Elektronik İmzanın İşleyişi

Ayşe kendi oluşturduğu bir elektronik postayı Barış'a güvenli bir şekilde ulaştırmak istemektedir. Ayşe'nin bir açık, bir de özel anahtarı vardır ve açık anahtarını Barış'a daha önceden ulaştırmıştır. Bu gönderim şu şekilde gerçekleşir:

1) Ayşe özel anahtarı ile metni şifreler, böylelikle metnin imzasını oluşturmuş olur (Şekil 8). Ayşe'nin özel anahatarı, Ayşe'den başkasında olmadığından ve başka bir anahtar kullanarak bu imzanın birebir aynısını oluşturmak mümkün olmadığından, üretilen bu imza bilgisi Ayşe'ye özeldir.



Şekil 8 Elektronik İmzanın Oluşturulması

2) Ayşe imzalı metni Barış'a gönderir.

2) Barış, Ayşe'nin açık anahtarını kullanarak imzayı onaylama işlemini gerçekleştirir (**Error! Reference source not found.** - 1. adım). Ortaya çıkan onaylanmış imza metni ile düz metin aynı ise imza doğrulanmış olur (**Error! Reference source not found.** - 2. adım).

Şekil 9 Elektronik İmzanın Onaylanması

Buradaki senaryoda, Ayşe, imza bilgisini düz metnin sonuna ekleyerek Barış'a gönderdi. Barış, Ayşe'nin elektronik imzasını onayladıktan sonra şu sonuçlara varabilir:

- "Düz metin değiştirilmeden bana ulaştı"
- "Metnin elektronik imzası Ayşe'nin açık anahtarı ile doğrulandı. Demek ki bu imza Ayşe'den başkası tarafından atılmış olamaz. Öyleyse mesajı gerçekten Ayşe gönderdi"
- "Daha sonra Ayşe bana gönderdiği bu mesajı göndermediğini iddia ederse, ona yalnızca kendisi tarafından özel anahtarını kullanarak oluşturulabilecek elektronik imzasını gösterebilirim"

Şifrelemede genel olarak, şifrelenecek/imzalanacak metnin boyu ne kadar artarsa, işlem süresi de ona bağlı olarak artar. İmzalanacak metnin boyu büyüdükçe de imzalama süresi ona bağlı olarak dramatik bir şekilde yükselir. Pratik uygulamalarda açık anahtar algoritmaları uzun metinlerin imzalanmasında, imzalama süresinin saniyeler hatta dakikalar alması nedeniyle başarım açısından çok yetersiz kalmaktadır. Metin boyutlarının çok değişken olması imzalama sürecinin ne kadar zaman alacağına ilişkin net bir tahmin yapılmasını engellemektedir. Buna ek olarak, imzalanacak veri ile elektronik imza aynı boydadır. Yani elektronik imza verisinin boyu, imzalanan verinin boyuna eşittir. Yukarıdaki örnekte olduğu gibi düz metnin doğrudan imzalanması, iletim hattının iki kat daha fazla kullanılmasına neden olacaktır.

Bu iki problemi çözmek ve başarımı arttırmak için elektronik olarak imzalama yapılmadan önce **tek-yönlü özet algoritması** (Hash) kullanılarak metnin sabit uzunlukta bir özeti üretilir. Özet algoritmaları metnin boyu ne olursa olsun sabit uzunlukta bir çıktı üretmektedir.

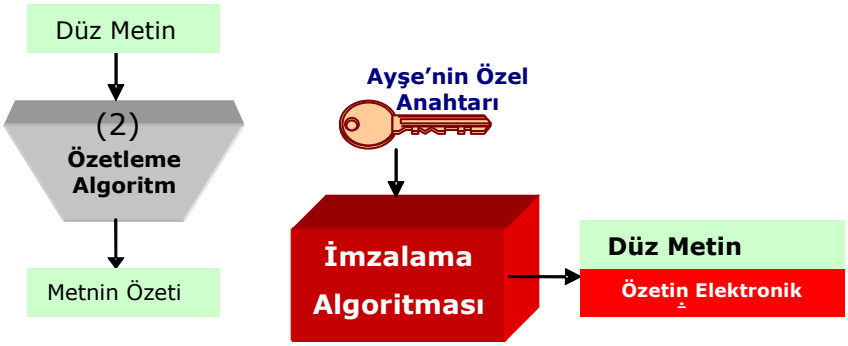
Yukarıdaki senaryoyu özetlemeyi de içine alacak şekilde şöyle değiştirebiliriz:

1. Ayşe gönderilecek metni tek-yönlü özet fonksiyonundan geçirir ve metnin boyundan bağımsız olarak ancak metnin karakterini içerecek şekilde sabit uzunluklı bir özet oluşturmuş olur (**Error! Reference source not found.** – 1. adım).

2. Ayşe tek-yönlü fonksiyon çıktısını özel anahtarı ile şifreler. Böylece metnin elektronik imzasını oluşturmuş olur (**Error! Reference source not found.** – 2. adım).

3. Ayşe metnin sonuna 2. adımda oluşturduğu metnin elektronik imzasını ekleyerek Barış'a gönderir.

(1)



Şekil 10 Elektronik İmzanın Metnin Özeti Alınarak Oluşturulması

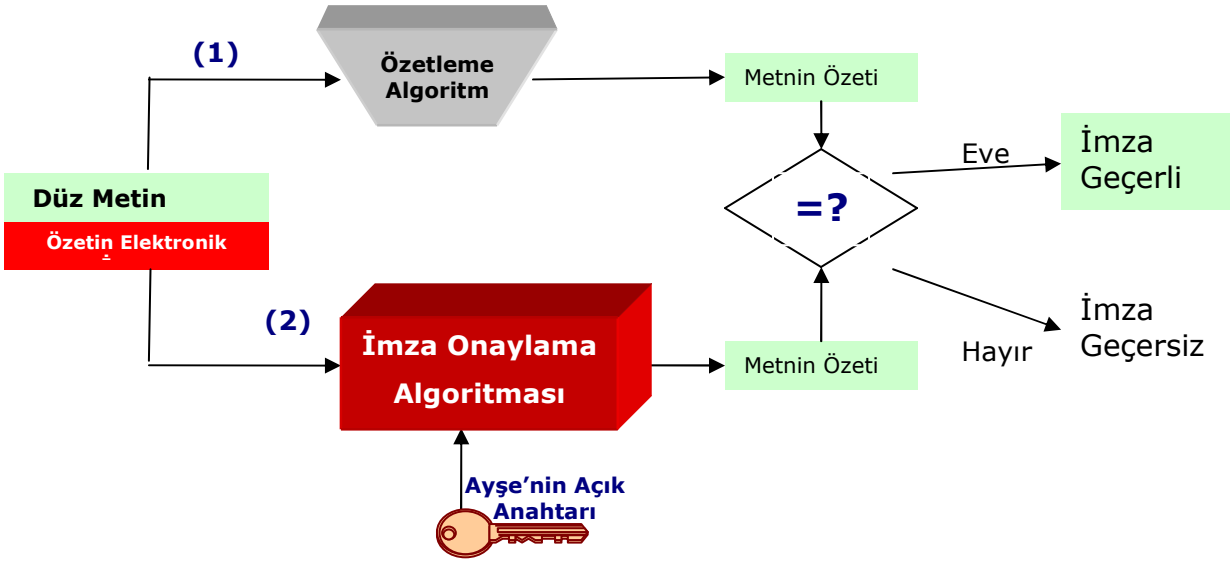
4. Barış Ayşe'nin gönderdiği düz metnin tek-yönlü fonksiyon ile özetini üretir (

5.

6. Şekil 11 - 1. adım). Ardından, imza onaylama algoritmasını kullanarak, Ayşe'nin açık anahtarıyla bu metnin elektronik imzasının şifresini çözer (

7.

8. Şekil 11 – 2. adım). Eğer 1. adım ve 2. adımda elde edilen sonuçlar birbirinin eşi ise, metnin elektronik imzası geçerli anlamın gelir.



Şekil 11 Elektronik İmzanın Onaylanması

2.3 Açık Anahtar Altyapısı

Elektronik İmza'nın kullanılması için elverişli bir ortam sağlayan açık anahtarlı şifreleme yöntemleri, hedeflenen güvenlik gereksinimlerini karşılamakla birlikte bir takım zorluklara da sahiptir. Bunlar kısaca şöyle özetlenebilir:

- Anahtar çiftlerinin üretimi
- Anahtarla sahibinin eşleştirilmesi
- Anahtarların tanınması
- Özel anahtarın korunması
- Farklı uygulamalarda aynı imzanın kullanılabilmesi

Yukarıda sıralanan sorunlara çözüm getirmek, açık anahtarlı şifreleme yöntemlerinin kullanımı yoluyla yukarıda bahsedilen bütünlük, kimlik doğrulama ve inkâr edilmezlik hizmetlerini kullanıcılara vermek ve elektronik imza teknolojisinin kolay kullanımını sağlamak için gerekli teknoloji, standart, yasa, yönetmelik, kuruluş, ürün ve hizmetlerin bütününe "*Açık Anahtar Altyapısı (AAA)*" denir.

AAA'nın temel bileşenleri şunlardır:

Elektronik sertifikalar: Kişinin kimlik bilgileriyle açık anahtarını birbirine bağlayan elektronik kayıttır. Sertifika için genel olarak Uluslararası Telekomünikasyon Birliği'nde (ITU) geliştirilen X.509 standardı kabul görmektedir. Elektronik sertifika sayesinde, kişilerin elektronik anahtarlara sahip olması sağlanır. Elektronik sertifika, sanal ortamdaki kimlik kartımızdır.

Elektronik sertifika hizmet sağlayıcısı: Elektronik sertifikada yer alan bilgilerin doğruluğundan emin olunması için bir güven modeline ihtiyaç duyulmaktadır. Elektronik imza yasasında tanımlanan elektronik sertifika hizmet sağlayıcılar (ESHS), sertifika veren kuruluşlar olarak tanımlanmaktadır. ESHS, güven ve itibarın tesisi için belirlenmiş kurallara bağlı olarak faaliyetlerini yürütmek ve yasa

ile belirlenen bir kuruluş tarafından denetime açık olmak zorundadır. Türkiye'de ESHS faaliyetlerini düzenleyici kurum olarak Telekomünikasyon Üst Kurulu (TK) görevlendirilmiştir.

Elektronik imza algoritmaları: Elektronik imza üretmek ve bir elektronik imzanın doğruluğunu onaylama için kullanılan karmaşık matematiksel fonksiyonlar grubudur. Bu algoritmalara örnek olarak RSA, EC, SHA-1, MD5 verilebilir.

Güvenlik protokolleri: Elektronik imzanın, uygulamaların bir parçası olarak kullanılmasını sağlayan iletişim kuralları dizisidir. Örneğin, SSL (secure socket layer) Web sunucusuyla İnternet tarayıcısı arasında çalışan ve güvenli haberleşme sağlayan açık anahtar altyapısı temelli bir iletişim protokolüdür.

Uygulamaya ilişkin diğer standartlar: Anahtarların saklanması, değiştirilmesi, elektronik imzanın oluşturulması, taşınması konularıyla ilgili oluşturulmuş standartlardır. Bugün RSA Laboratuvarları öncülüğünde geliştirilmiş olan PKCS ("public key cryptography standards" – açık anahtar kriptografisi standardları) geniş kabul gören ve kullanılan standardlardan biridir.

Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları: Anahtarların ve sertifikanın güvenlik içinde taşınması ve elektronik imza oluşturmak ve doğrulamak amaçlarıyla kullanılan USB çubuk (token), akıllı kart (smart card) ve akıllı kart okuyucular gibi cihazlardır (Bkz. Bölüm 6)

ESHS'nin çalışma ilkeleri ve esasları ve yönetmelikler: ESHS'ler, çalışma ilkelerinin ve kurallarının ne olduğunu ve bu ilke ve kurallara uygun olarak faaliyetlerini nasıl yerine getirdiklerini yayınladıkları belgelerle açıklarlar. Ayrıca TK, hizmet sağlayıcılarının uyması gereken kuralları yönetmeliklerle düzenler.

Bir AAA'nın sağlıklı bir şekilde işleyişi, yukarıda özetlenen bileşenlerin birbirleriyle uyum içinde çalışmasına bağlıdır.

3 Elektronik Sertifika Hizmet Sağlayıcının Görevleri

Bu bölümde bir Elektronik Sertifika Hizmet Sağlayıcı'nın (ESHS) yasal olarak yerine getirmesi gereken görevlere ilişkin bilgiler verilmiştir. Yasaya göre ESHS şöyle tanımlanmaktadır (Madde 8):

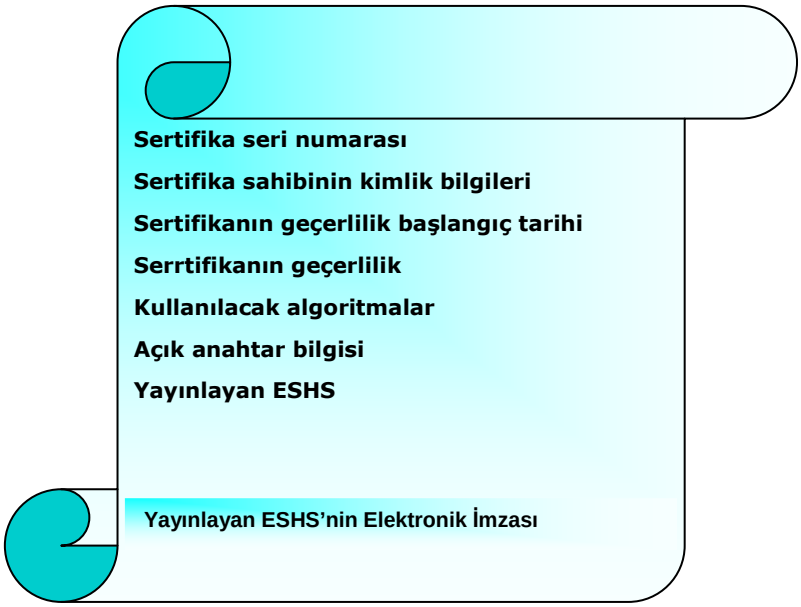
"ESHS, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum kurum ve kuruluşları ile gerçek veya özel hukuki tüzel kişilerdir."

Elektronik imzanın tanımı Bölüm 2'de verilmişti. Bu bölümde de öncelikle yasada tanımlanan elektronik sertifika, zaman damgası hakkında gerekli bilgiler verilmiştir.

3.1 Elektronik Sertifika

Bir ESHS'nin temel görevi elektronik sertifika yayınlamaktır. Yasada elektronik sertifika şöyle tanımlanır (Madde 3ı): "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı".

Bir elektronik sertifika, kullanıcı kimliği ile kullanıcı için üretilen imza doğrulama verisini, yani kullanıcının açık anahtarını birbiri ile ilişkilendiren bir veri yapısıdır. Bu özelliği ile elektronik sertifika kullanıcıların sanal ortamdaki kimlik kartı olarak nitelendirilebilir.



Elektronik Sertifika, bir ESHS tarafından yayınlanır. Temel olarak bir elektronik sertifika içinde yer alan bilgiler **Error! Reference source not found.**'de belirtilmiştir. Aşağıda bu bilgilerin kısa açıklamaları verilmiştir:

Şekil 12 Elektronik Sertifika

Sertifika seri numarası: Yayınlayan tarafından üretilen sertifikaya ait tekil kimlik numarasıdır.

Sertifika sahibinin kimlik bilgileri: Sertifika sahibini tekil olarak tanımlayabilen kimlik bilgileri. Bu bilgilere örnek olarak T.C. Kimlik Numarası, isim, soyad, e-posta bilgileri verilebilir.

Sertifika geçerlilik başlangıç tarihi: Sertifika belirtilen bu tarihten önce kullanılamaz.

Sertifika geçerlilik sonlanma tarihi: Sertifika belirtilen bu tarihten sonra kullanılamaz.

Sertifikanın kullanım amacı: Bu sertifika ve içinde yer alan açık anahtar bilgisinin ne amaçla kullanılmak üzere yayınlandığı belirtilir. Bir sertifika, örneğin, elektronik imzalama, şifreleme, kimlik doğrulama gibi amaçlarla kullanılabilir.

Kullanılacak algoritmalar: Bu açık anahtar bilgisinin hangi algoritmalarla birlikte kullanılabileceği yazılır. Örnek olarak RSA, DSA, EC, DH verilebilir.

Açık anahtar bilgisi: Bu sertifikada kimliği tanımlanan kullanıcıya ait açık anahtar.

Yayınlayan ESHS: Bu sertifikayı yayınlayan ESHS'nin kimlik bilgileri.

Yayınlayanın elektronik imzası: Bu sertifikayı yayınlayan ESHS, sertifika bilgilerini kendi özel anahtarını kullanarak imzalar. Bu sertifikayı kullanacak bir kullanıcı, imzayı ESHS'nin açık anahtarı ile onaylayarak, gerçekten belirtilen ESHS tarafından yayınlandığından emin olur.

Yukarıda özellikleri belirtilen bir elektronik sertifikanın yasal olarak geçerli olan güvenli elektronik imza oluşturmak amacıyla kullanılabilmesi için, yasada tarif edilen "Nitelikli Elektronik Sertifika" özelliklerine sahip olması gerekir.

3.2 Nitelikli Elektronik Sertifika

5070 sayılı Kanun uyarınca gereken şartları sağlayan ve TK tarafından yetkilendirilmiş nitelikli bir ESHS tarafından verilmiş sertifikalardır. Nitelikli elektronik sertifikalar ITU-T Rec. X.509V.3 standardına uymak zorundadır (Tebliğ Madde 5). Buna göre bir nitelikli elektronik sertifikada yer alması zorunlu olan bilgiler şunlardır (Madde 9):

- Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare
- ESHS'nin kimlik bilgileri ve kurulduğu ülkenin adı
- İmza sahibinin teşhis edilebileceği kimlik bilgileri
- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi (yani kullanıcının açık anahtarı)
- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri
- Sertifikanın seri numarası
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi
- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri
- Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgiler
- ESHS'nin sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası

•

3.3 Zaman Damgası

Özellikle belirli bir son işlem tarihi olan vergi beyannamesi vermek, fatura ödemesi yapmak gibi işlemlerde, elektronik hizmetten once son gün beyannamesini vermeyen ya da ödemesini yapmayan rahatlıkla tespit edilebilirdi. Çünkü vergi dairesi ya da bankalar belli bir saatte kapanırlardı. O saate kadar da işlemi gerçekleştirmeyen yükümlüler geç kalmış sayılırdı. Ancak elektronik ortamda gerçekleşen işlemlerde alıcının saati ile göndericinin saati birbirinden farklı olabilir. Bu nedenle işlemin gerçekleştiği tam saatin bilinmesi bir gereklilik halini almıştır. Elektronik bir veriye, bu veriye ilişkin tarih/saat bilgisinin güvenilir bir kaynaktan edinilerek eklenmesine "Zaman Damgası" denir. Yasaya göre Zaman Damgası şöyle tanımlanmıştır (Yasa Madde 3h):

"Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespiti amacıyla, ESHS tarafından elektronik imza ile doğrulanan kaydı."

Buna gore ESHS'nin temel görevlerinden biri de kullanıcılara zaman damgası hizmeti vermektir. ESHS bu hizmeti verirken bir takım uluslararası standardlara uygun olarak vermekle yükümlüdür. (Tebliğ Madde 10)

Ayrıca ESHS zaman damgası hizmetlerini vermesi ile ilgili ilke ve uygulama esaslarının belirtildiği belgeleri yayınlamakla yükümlüdür.

Kullanıcının bu hizmeti almak için ESHS'den talep etmesi gerekir (Yönetmelik Madde 31).

3.4 Elektronik Sertifika Hizmet Sağlayıcısı

Yasaya göre Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir (Yasa Madde 8).

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

- Güvenli ürün ve sistemleri kullanmak,
- Hizmeti güvenilir bir biçimde yürütmek,
- Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Her sertifika hizmet sağlayıcısı, çalışma ilkesi ile ilgili ayrıntılı bilgilerin bulunduğu Sertifika Uygulama Esasları (SUE) ve Sertifika İlkeleri (Sİ) adlı belgeleri yayınlamalıdır.

3.5 ESHS'nin Yükümlülükleri

TK tarafından nitelikli sertifika vermek üzere yetkilendirilen ESHS'lerin yükümlülükleri şunlardır (Madde 10):

- Hizmetin gerektirdiği nitelikte personel istihdam etmek
- Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere dayanan güvenilir bir biçimde tespit etmek

- Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemek
- İmza oluşturma verisinin ESHS tarafından veya sertifika talep eden kişi tarafından ESHS'ye ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya ESHS'nin sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamak
- 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 bilgilendirmek
- Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmek
- Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamak
- Faaliyetine son vereceği tarihten en az üç ay önce durumu TK'na ve elektronik sertifika sahibine bildirmek

ESHS'ye yüklenen yukarıdaki yükümlülükler ile yasa şunları garanti etmektedir:

- İmzası doğrulanan şahıs, gerçekten kimliği belirtilen şahıstır.
- ESHS'nin faaliyetleri sonlansa bile, ondan elektronik sertifika almış kişilere hizmetin devamlılığını sağlamak için gerekli önlemler alınmıştır.
- Kullanıcının, kullanım konusunda bilinçlendirilmesi sağlanmıştır.

ESHS, üretilen imza oluşturma verisinin (yani sertifika sahibinin özel anahtarının) bir kopyasını alamaz veya bu veriyi saklayamaz. Bu demektir ki ESHS sadece nitelikli elektronik sertifikanın yayınlanma aşamasında devreye girer. Bir ESHS'nin yaptığı iş esas olarak, kendisi tarafından verilmiş nitelikli elektronik sertifikayı kullanan imza sahibinin kimliğini tarafsız 3. şahıs sıfatıyla doğrulamaktır. Bu sertifikayı kullanarak gerçekleşen güvenli iletişim yalnızca iletişime katılan tarafları ilgilendirir.

3.6 Sunucu Sertifikası

Sunucu sertifikaları, Web sunucularının kimlik bilgilerini ve açık anahtarını taşıyan ve bu sunuculara bağlanan kullanıcılara sunulan elektronik sertifikalardır. Özellikle son dönemlerde artan ve ülkemizde de görülen internet üzerinden dolandırıcılık faaliyetlerinin bir kısmı, gerçeğine çok benzeyen taklit Web siteleri aracılığı ile gerçekleştirilmektedir. Sunucu sertifikaları ile bağlanılan web sitesinin kimliği güvenilen bir ESHS aracılığı ile doğrulanabilir.

Sunucu sertifikası, kişisel sertifikalar gibi X.509 standardına uygun üretilirler. Bu sertifika sayesinde, bağlanılan Web sunucusunun, kullanıcılar açısından kimlik doğrulaması yapılmış olur. Bu yöntemde kullanıcı, bağlandığı web sitesinde hiçbir işlem yapmadan önce sunucu sertifikasının doğruluk sınamasını gerçekleştirir. Sertifikadaki sunucu kimlik bilgisi, sertifika geçerlilik süresi gibi bilgiler elle kontrol edilir. Bunun yanında, en önemlisi, bu sertifikanın TK tarafından yetkilendirilmiş bir ESHS tarafından yayınlanıp yayınlanmadığına bakılır.

İsteğe bağlı olarak, bu kimlik doğrulaması çift taraflı olarak gerçekleşebilir. Bu yöntemle hem Web sunucusu, karşısındaki kullanıcının kimliğinden hem de kullanıcı

Web sunucusunda emin olabilir. Bu kimlik doğrulama işleminde bugün yaygın olarak kullanılan yöntem, aynı zamanda kullanıcı ile Web sunucusu arasında şifreli haberleşmeye de olanak tanıyan SSL protokolüdür.

3.7 Sertifika İlkeleri ve Sertifika Uygulama Esasları

ESHS tarafından yayınlanması zorunlu olan bir belgelerdir (Tebliğ Madde 7). Sertifika İlkeleri, sertifika kullanımı, sertifika yaşam çevrimi ile ilgili kurallar listelenir. ESHS, elektronik sertifikalar ve kurduğu AAA ile ilgili tüm iş sürecini bu belge ile tanımlar.

Sertifika Uygulama Esasları'nda, Sertifika İlkeleri belgesinde belirtilen kuralların nasıl uygulanacağı ayrıntılı bir biçimde ifade edilir. Genellikle Sertifika Uygulama Esasları, Sertifika İlkeleri'ne göre daha uzun, kapsamlı ve teknik bilgiler içeren bir belgedir.

ESHS, bu iki belgeyi IETF RFC 3647'ye uygun olarak hazırlamalıdır.

3.7.1 Elektronik Sertifikaların Kullanım Süresi

Her elektronik sertifikanın belli bir kullanım süresi vardır. Bir kişi için bir ESHS tarafından yayınlanan elektronik sertifika, sertifika sahibi tarafından hayatı boyunca kullanılamaz. Sertifikanın kullanımının bir başlangıç bir de bitiş süresi vardır. Elektronik imza uygulamaları, elektronik sertifikalarla işlem yapmadan önce sertifikanın geçerlilik süresini kontrol ederler. Genellikle bu süre bir yıldır.

ESHS'nin sertifikasının da bir geçerlilik süresi vardır. Bu süre 10 yılı aşamaz. (Yönetmelik Madde 18)

3.8 Sertifika Yaşam Çevrimi

Bir sertifikanın üretilmesinden iptaline kadar geçirdiği aşamalara "Sertifika Yaşam Çevrimi" denir. Bu çevrim, ESHS tarafından net bir şekilde Sertifika İlkeleri ve Sertifika Uygulama Esasları belgeleri içinde tanımlanır. Aşağıda bir sertifika yaşam çevrimi, genel hatlarıyla tarif edilmiştir. Gerçek uygulamalarda bazı farklılıklar olabileceği unutulmamalıdır.

3.8.1 Sertifikanın Yayınlanması

1. Kullanıcı, elektronik sertifika almak için ESHS'ye başvurur. Bu başvuru adımında, kimlik doğrulamanın güvenliği için yüzyüze görüşme gereklidir.
2. ESHS, kullanıcının kimliğini doğrular ve sertifikayı yayınlar.
3. ESHS, sertifikayı, herkese açık bir ortama (örneğin bir dizin hizmeti üzerine) aktarır.

3.8.2 Sertifikanın Kullanımı

1. Kullanıcı gerçekleştirdiği işlemi ya da göndereceği mesajı kendi özel anahtarı ile imzalar ve alıcıya iletir (**Error! Reference source not found.**).

2. Alıcı mesajı alır, mesajdaki sayısal imzayı göndericinin açık anahtarıyla doğrulaması gerekir. Bunun için kullanıcının nitelikli elektronik sertifikasını ESHS'nin herkese açık dizin hizmeti üzerinden sorgular ve sertifikayı elde eder.

3. Sertifikadaki geçerlilik süresini, nitelikli sertifika olup olmadığını ve imzalayan ESHS'nin imzasının doğruluğunu kontrol eder.

4. 2. ve 3. aşamadan sorunsuz geçildikten sonra, mesajdaki elektronik imzanın alıcıya ait olup olmadığını kontrol eder. Bunu imza onaylama işlemi ile gerçekleştirir (

5.

6. Şekil 11). İmza onaylanırsa alıcı, mesajı gönderinin kimliğinden, mesajın alıcıdan çıktığı şekliyle kendisine ulaştığından ve göndericinin bu mesajı gönderdiğini daha sonra inkâr edemeyeceğinden emin olur.

3.8.3 Sertifikanın İptali ve Askıya Alınması

Bir nitelikli elektronik sertifika, özel anahtarın kaybolması veya sertifikanın geçerlilik süresinin sonuna gelmesi durumlarında iptal edilebilir. Geçici süreyle kullanımdan kaldırılacak olan sertifikalar ise askıya alınır. İptal edilen sertifika tekrar kullanılamaz. Askıya alınan sertifika, askıda olduğu süre boyunca kullanılamaz. Ancak askıda olan bir sertifika askıdan indirildiğinde normal kullanımına devam edilebilir.

ESHS, iptal edilen sertifikaları Sertifika İptal Listesi (SİL) adında bir liste ile periyodik olarak yayınlar. SİL için genel kabul görmüş X.509 v2 standardı kullanılmaktadır. ESHS, aynı yayınladığı sertifikalarda olduğu gibi yayınladığı SİL'leri de elektronik olarak imzalar. Bir sertifika iptal edildiğinde, bir sonraki SİL içerisinde iptal edilen sertifikaya ilişkin bilgileri yayınlanır. Sertifikaların tutarlı bir şekilde kullanılabilmesi için SİL her kullanımda kontrol edilmelidir.

SİL'de üç tür sertifika yer alır:

- İptal edilen sertifikalar
- Geçerlilik süreleri dolan sertifikalar
- Geçici olarak kullanımdan kaldırılan (askıya alınan) sertifikalar

3.9 Kök Sertifika

ESHS'nin elektronik sertifikasına **kök sertifika** denir. ESHS'nin, kendisinden elektronik sertifika alan kullanıcılar gibi bir çift anahtarı vardır. Bu anahtarlardan özel anahtar, yayınlanan elektronik sertifikaları imzalamak için kullanılır. ESHS'nin açık anahtarı ise ESHS'nin kök sertifikası içinde yer alır ve kullanıcılar tarafından bu ESHS'nin yayınladığı elektronik sertifikalara attığı elektronik imzasının doğrulanması için kullanılır. Bir nitelikli elektronik sertifika, ancak yayınlayan ESHS'nin sertifika üzerindeki imzası geçerliyse kullanılabilir (**Error! Reference source not found.**). Bir nitelikli elektronik sertifikaya ulaşan bir kullanıcı, öncelikle bu sertifikanın geçerliliğini, sertifika üzerindeki ESHS imzasının geçerliliğini kontrol ederek sınar Kök sertifika açık anahtarın ESHS'nin olduğunu onaylar.

ESHS'nin özel anahtarı, bir AAA sistemindeki güven zincirinin en önemli halkasıdır. ESHS'nin özel anahtarı, yetkisiz bir kullanıcının eline geçerse, AAA

üzerinde verilen tüm güvenlik hizmetleri ve kurulan güvenli iletişim altyapısı tehlikeye düşer. Bu nedenle ESHS'nin özel anahtarını saklamak için özel ve yüksek güvenlik içeren saklama ortamları kullanılır. Küçük bir kutuya benzeyen ve yalnızca yetkili kullanıcıların ve programların erişmesine izin verecek şekilde ESHS'nin özel anahtarını saklayan bu cihazlara Donanım Güvenlik Modülü (Hardware Security Module) denir.

3.10 Elektronik Sertifikaların Uygulama Alanları

Elektronik imza ve buna bağlı olarak elektronik sertifikalar, sağladıkları güven altyapısı sayesinde kendisine birçok uygulama alanı bulmuştur. Bu alanlardan bazıları şöyle özetlenebilir.

- **Bütünlük, Kimlik Denetimi ve İnkar Edememezlik Hizmetleri:** Kurumlar mesajların doğru kişi tarafından, içeriği değiştirilmeden ve karşı tarafın inkar edemeyeceği şekilde iletimini sağlamak için elektronik sertifikalar kullanırlar. Yasa ile nitelikli elektronik sertifikalar yalnızca bu gereksinimleri karşılamak amacıyla yayınlanabilir ve kullanılabilir.
- **Erişim Denetimi:** Bilgisayar sistem ve terminallerine, İnternet sitelerine, kurum içi ağ üzerindeki hizmetlere erişim denetimini sağlamak amacıyla kullanılırlar.
- **Belge İletiminin ve İletim Zamanının İspatı:** Kritik belgelerin hukusal açıdan zamanını ve tarihini doğrulamak için elektronik imza yasası ile birlikte gelen zaman damgası hizmeti kullanılabilir.
- **Elektronik İş Akışı:** Kağıt üzerinde işleyen bürokrasi, ıslak imza yerine geçebilen güvenli elektronik imza sayesinde elektronik ortamda çok daha hızlı, düşük maliyetli ve güvenilir bir şekilde gerçekleştirilebilir.
- **Resmi başvuru işlemleri**: Bu işlemler, devlet dairesine gitmeden, zaman kaybetmeksizin, bilgisayar başından gerçekleştirilebilir. İşlemlerin sonuçları da aynı yolla izlenebilir.
- **Arşivleme:** Depolanmış elektronik belgelere ya da mesajlara erişildiğinde, belgenin değiştirilmeden orijinal haliyle saklandığından emin olunması amacıyla kullanılabilir.

3.11 Secure Sockets Layer (SSL)

İnternet üzerindeki iletişimlerde kimlik doğrulaması ve şifreli veri iletimi için Netscape Communications tarafından tasarlanmış iletişim protokolüdür. En yaygın kullanımı alanı Web sunucuları ve tarayıcıları arasındaki iletişimin güvenli hale getirilmesidir.

Kimlik doğrulama işlemi için elektronik sertifikalar kullanılmaktadır. Şifreleme, kimlik doğrulama ve veri bütünlüğü kontrol özellikleri, ihtiyaca göre hem sunucu hem de istemci tarafında gerçekleştirilmek üzere ayarlanabilir. Örneğin, yalnız sunucunun kimliğinin doğrulanması için SSL protokolü aracılığı ile sunucu sertifikasının tarayıcıya iletilmesi kontrol için yeterlidir.

3.12 Elektronik Sertifika Hizmet Sağlayıcılı ile Noterlerin Farkı

Elektronik Sertifika Sağlayıcılığı ile noterler arasında bir takım benzerlikler bulunmakla beraber aslında hizmet yapılarında farklılıklar bulunmaktadır. Noterler, bir işlemin vaki olduğunun resmi kaydını zaman mührüyle birlikte tutarlar. Bu anlamda işleme ve/veya kişilere güvenilir tanık durumundadırlar. Örneğin noterde bir

sözleşme yapıldığında, noter açısından sözleşme içeriğinin hukuki boyutları önemli değildir. Önemli olan, evrakın ilgili taraflarca belirtilen tarihte noterin huzurunda ve tanıklığında imzalandığıdır. Noterin kimlik tespiti de beyan usulünde çalışır. Kimliği doğrulamak yerine evraktaki kimlikle kişinin beyan ettiği kimlik belgesini karşılaştırır. Bir noter, noterlik hizmeti alan bir vatandaşla daha önce çalışmış olmak zorunda değildir.

Kimlik doğrulamada ESHS, noterde olmayan bir sorumluluk taşımaktadırlar. ESHS, işlemi gerçekleştiren şahsın kimliğin doğruluğunu da kontrol eder. Bununla birlikte gerçekleştirilen işlemle ilgisi yoktur. Gerçekleştirilen işlem veya gönderilen belge tamamen iletişim kuran tarafları ilgilendirir. ESHS, bu iletişimde güven altyapısının oluşmasını sağlayan ve iletişimin temel güvenlik gereksinimlerine uygun bir biçimde çalışır. ESHS, bir kimyasal tepkimede, uygun ortam şartlarını sağlayan bir katalizör gibi görev yapar.

İletişim esnasında, elektronik imzanın onaylanması aşamasında sertifikanın geçerliliğinin kontrolüne ihtiyaç duyulabilir.

Ayrıca belgeye eklenmek üzere zaman damgası hizmeti alınabilir. Bu hizmet, belgeyi görmeden zaman bilgisinin belgeye iliştirilmesi olarak düşünülebilir. Bu işlemde de ESHS, tam olarak noter gibi davranmaz. Çünkü noter, noterlik hizmeti alınan belgenin bir kopyasını alır, içini görür, yapılan sözleşmenin/anlaşmanın miktarına bağlı olarak bir hizmet bedeli ve devlet adına damga vergisi alır. Bununla birlikte ESHS belgenin içeriği ile ilgilenmez. Ancak mesaj sahibi, mesajı imzalamakta kullanacağı nitelikli elektronik sertifika için ya da zaman damgası hizmeti için ESHS'ye bir ücret ödediğinden, dolaylı olarak da olsa bir ücretlendirme söz konusudur.

ESHS belgenin içeriği ile hiç ilgilenmez sadece belgenin gönderenin gönderdiği gibi alıcıya ulaştırılmasını yani değiştirilmediğini ve inkar edilemeyeceğini garanti eder. Öte yandan, noter huzurunda yapılan diğer pek çok işlemin (alım-satım işlemleri, vekaletler, ve benzeri) yasal olarak elektronik işlem çeklinde gerçekleşmesi mümkün değildir. Çünkü yasaya göre, kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri işlemleri elektronik imza ile gerçekleştirilmesi mümkün değildir (Yasa Madde 5).

Kısaca, hem işlevsel olarak hem de Türk Hukuku açısından, noterler ile ESHS'ler birbirine benzer ve farklı yanları olan ve birbirlerini tamamlayan işlevlere sahip iki kurum gibi düşünülmelidir.

3.13 ESHS'lerin Yetkilendirilmesi

Yasaya göre ESHS'ler faaliyete geçmek üzere TK'na bildirimde bulunurlar. Düzenleyici kurum olan TK, bildirim yapan ESHS üzerinde yaptığı denetimlerde yasada belirtilen şartların sağlandığına kanaat getirdikten sonra, bekleme süresinin sonunda ESHS çalışmaya başlamaktadır. Bu süreç ayrıntılı olarak aşağıda tarif edilmiştir:

1. **Bildirimin Yapılması:** Kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri, ESHS olma talebini, gerekli bilgi ve belgeleri eksiksiz olarak TK'na ibraz etmek suretiyle bildirimde bulunur.
2. **Bildirimin İncelenmesi ve Sonuçlandırılması:** TK, yapılan bildirim üzerindeki incelemesini iki ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki ay sonra faaliyete geçer. Tk,

ESHS'nin gerekli şartları sağlamadığını tespit ederse ESHS'ye ek süre verir. Eksiklerini verilen süre içerisinde gidermeyen ESHS, ESHS olma vasfını kaybeder.

3. **Bildirimdeki Değişiklikler:** ESHS, faaliyete geçtikten sonra, yapmış olduğu bildirimde herhangi bir değişiklik meydana gelmesi halinde, bu değişiklikleri 7 gün içinde TK'na bildirir.

3.14 ESHS'den Bildirimde İstenen Belgeler

ESHS olmak isteyenler aşağıdaki bilgi ve belgeleri TK'na sunmakla yükümlüdür:

- İletişim bilgileri
- Şirket ile ilgili belgeler
- Personel bilgileri
- Sertifika İlkeleri ve Sertifika Uygulama Esasları
- Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları
- Kendi Sertifikasının Örneği
- Sertifika Mali Sorumluluk Sigortası
- Sözleşme Örneği
- Hizmet Sözleşmesi
- Tebliğ ile istenilenler:
  - Yönetmelik ve Tebliğlerde belirlenen gereklilikleri sağlayacak, fiziki, personel, iletişim, donanım ve yazılım altyapısına sahip olmak
  - Türkiye'de yerleşik olarak AAA kurmuş olmak
  - Sertifika ve zaman damgası hizmetlerini, hazırlamış olduğu Sertifika İlkeleri ve Sertifika Uygulama Esasları dokümanlarına göre verebiliyor olmak
  - BS 7799-2 standardına uyumluluk belgesi sahibi olmak
  - Mali sorumluluk sigortası başta olmak üzere, hizmet aldığı taraflarla uygun sözleşmeleri imzalamış olmak

4 ESHS'nin Nitelikleri

Bölüm 0'de bir ESHS'nin ne olduğu ve nasıl işlediği anlatılmıştı. Bu bölümde ise yasa ve yönetmelikler gereği ülkemizde kurulacak ESHS'lerin ne tür niteliklere sahip olacağından bahsedilecektir.

4.1 Süreklilik

Gerek kamuya hizmet veren KSM gerekse ticari ESHS'ler,verdikleri hizmetler bakımından kesintisiz hizmet vermesi gereken bir kurumdur. Gerek özel gerekse kamu sektöründeki uygulamalarda, ESHS'lerden 7 gün 24 saat kesintisiz hizmet ihtiyacı olacaktır. Bunun yanında ESHS'nin kök sertifikasını, sertifika başvuru bilgilerini koruması ve saklaması ile ilgili kriterlere uygun davranması da önemli bir gereksinimdir.

4.2 ESHS'nin uyacağı Kriterler, Standardlar, Parametreler

Hizmet verecek olan ESHS'lerin kullanabilecekleri kriptografik fonksiyonlar ve parametreler ile ilgili sınırlamalar açıkça tarif edilmiştir (Tebliğ Madde 5,6,7,8,9, 10). Bu nitelikler şunlardır:

- ESHS'nin işleyişi ile ilgili sağlayacağı standardlar (Bkz Tebliğ Madde 9)

- İmza oluşturma ve doğrulama verileri (yani özel ve açık anahtarlar)
- Sertifika ilkeleri ve Sertifika Uygulama Esasları (Bkz. Bölüm 3.7)
- Kullanılacak güvenli elektronik imza oluşturma ve doğrulama araçlarının uyacağı standardlar (Bkz. Bölüm 6)
- ESHS'nin uyacağı güvenlik kriterleri (Bkz. Tebliğ Madde 11)

Kriptografi çok hızlı ilerleyen bir bilim dalıdır. Bu nedenle bugün güvenli sayılan bir algoritma bir sene sonra güvensiz hale gelebilir. Bu nedenle örneğin Tebliğ'in 6. maddesinde belirtildiği üzere geçerli sayılan parametreler 31/12/2005 tarihine kadar geçerlidir. ESHS'ler belirtilen tarihten sonra TK tarafından yayınlanacak yeni parametrelere uygun olarak kendi altyapılarını güncellemek zorundadırlar.

4.3 ESHS'lerin Denetimi

Yasaya göre ESHS yetkisi alındıktan sonra TK, ESHS'leri bu niteliklerin devamlılığını garanti etmek amacıyla denetlemeye devam edecektir. Bu nedenle yetki belgesine sahip olan ESHS, ancak sahip olduğu nitelikleri sürdürdüğü takdirde hizmet vermeye devam edebilecektir. Ancak kamu kurumlarına hizmet veren KSM bu kapsamın dışındadır.

5 Türkiye'deki ESHS Yapılanması

5.1 Kamudaki Yapılanma

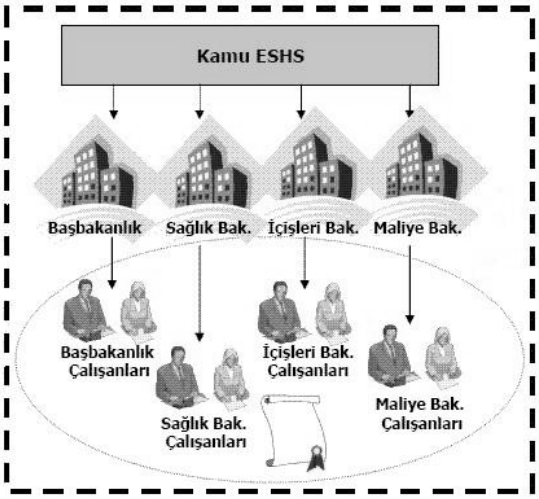
6 Eylül 2004 tarihinde yayınlanan ve 2004/21 numaralı Kamu Sertifikasyon Merkezi (KSM) oluşturulması konulu bir Başbakanlık Genelgesi yayınlanmıştır.

Genelge, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaları durumunda ortaya çıkacak sistemsel karmaşaya ve emek ve kaynak israfına engel olunmasını hedeflemektedir. Ayrıca, ulusal güvenlik gerekleri göz önünde bulundurularak KSM'de, ulusal yazılım ürünleri kullanılacağı belirtilmektedir.

Genelge ile istisnalar dışındaki hiçbir kamu kurumu, elektronik sertifika ihtiyaçlarını karşılamak amacıyla kendi bünyelerinde yeni bir yatırım yapmayacaktır. Kamu kurumları ve çalışanları, bu ihtiyaçlarını KSM'den temin edilecek elektronik sertifikalar ile karşılayacaklardır (Şekil 13). Bu konuda daha önceden başlamış olan ve devam eden çalışmalar durdurulacak, halihazırda kullanılmakta olan sistemler ise TK'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

Bunun sonucunda tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını, kamu kurumlarının kurum içi ve kurumlar arası elektronik sertifika ihtiyaçlarının karşılanmasını ve sertifika yaşam çevriminin yönetilmesini sağlayacak KSM, TÜBİTAK UEKAE bünyesinde oluşturulmuştur (www.kamusm.gov.tr). KSM, yetki belgesi almak üzere TK'na başvuruda bulunmuştur. Haziran 2005 ayı içerisinde sertifika dağıtımına başlaması beklenmektedir.

Kamu kurumlarının, KSM'den hizmet alması için kendi altyapılarının uygunlaştırılması için gerekli çalışmaları Devlet Planlama Teşkilatı (DPT) ile eşgüdümlü olarak yürüteceklerdir.



Şekil 13 Kamuda Sertifikasyon Yapılanması

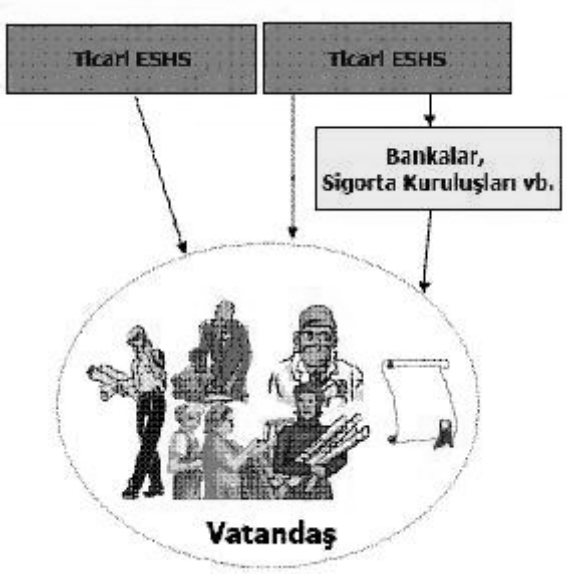
5.2 Özel Sektörde Yapılanma

Önümüzdeki zaman içerisinde kademeli bir şekilde, elektronik olarak verilmekte ve verilecek olan kamu hizmetlerinde vatandaşın elektronik imzası istenmeye başlanacaktır. Bu hizmetler sadece kamu kurumlarıyla sınırlı değildir. Örneğin bir özel banka da İnternet şubesinden hizmet almak isteyen müşterilerine nitelikli elektronik sertifika sahibi olma zorunluluğu getirebilir. Vatandaşların bu tür hizmetlerden yararlanabilmek için ticari ESHS'lerden birinden elektronik sertifika temin etmek zorundadır (Bkz. Şekil 14).

Yasanın ve yönetmeliğin çıkması ile ticari olarak ESHS hizmeti verecek olan kurumların TK'na başvuruları başlamıştır. TK'na ESHS hizmeti vermek üzere şu ana kadar başvuran kurumlar şunlardır:

- Egüven Elektronik Bilgi Güvenliği A.Ş.
- Türktrust Bilgi iletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Ticari ESHS olmak üzere başvuru yapmanın en son tarihi diye bir kavram söz konusu değildir. İsteyen her gerçek ya da özel hukuk tüzel kişileri, ESHS olmak üzere başvuruda bulunabilir.

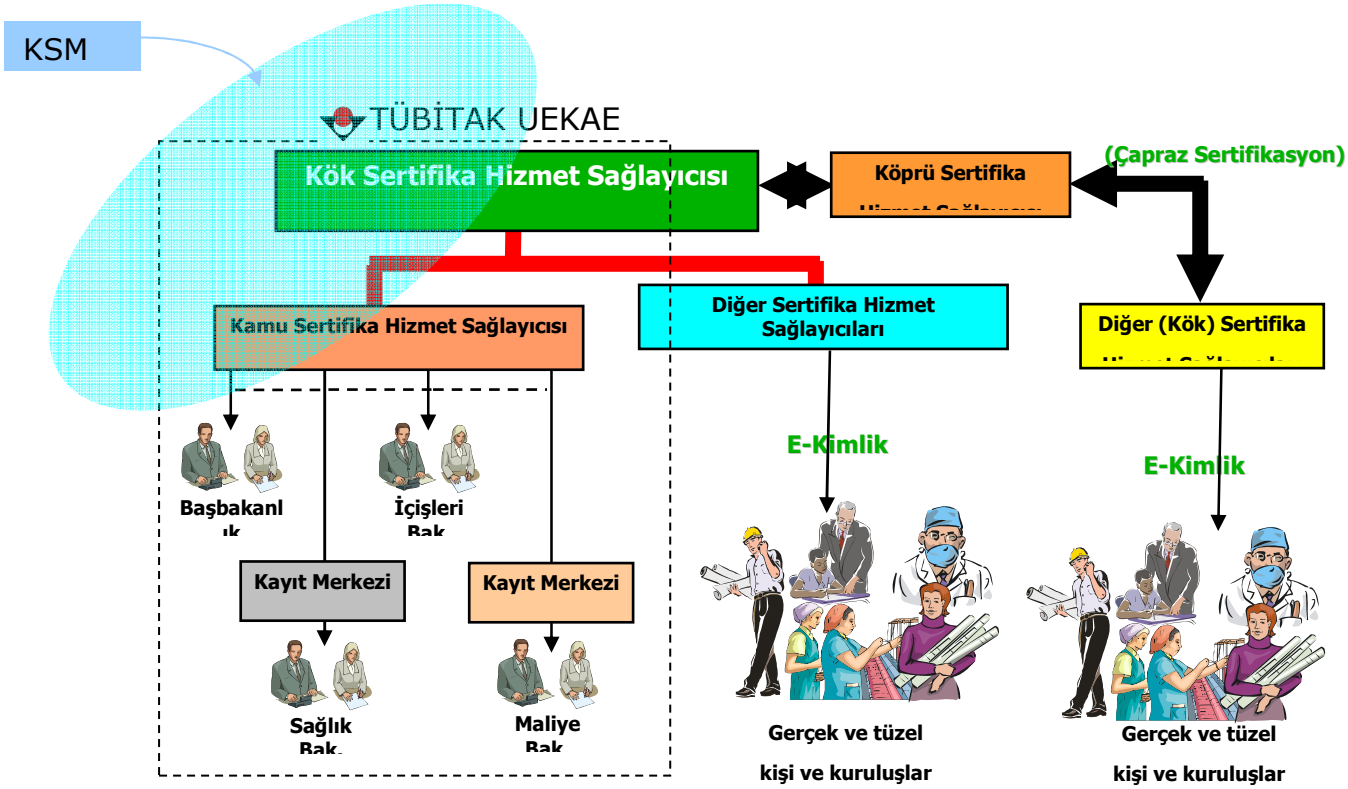


Şekil 14 Türkiye'de Ticari ESHS Yapılanması

TK'na ticari ESHS hizmeti vermek üzere başvuracak kurumlar yasa, tebliğ ve yönetmelikte belirtilen şartları sağlamak zorundadır.

5.3 Ayrıcalıklı Durumlar

KSM Kök Sertifika Hizmet Sağlayıcısı ile buna bağlı olarak Kamu Sertifika Hizmet Sağlayıcısı olarak hizmet verecektir. Yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet sistemlerini kendi bünyelerinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları, sertifikalarını, KSM'den temin edeceklerdir (Bkz. Şekil 15).



Şekil 15 Türkiye'deki ESHS Yapısı

5.4 Avrupa Birliğinde Durum

Avrupa Birliği'ne üye tüm ülkelerde elektronik imzaya yönelik olarak yayınlanmış olan 1999/93/EC direktifi yerine getirilmiştir. İrlanda hariç 14 üye ülkede en az bir nitelikli sertifika üreten ESHS vardır. Fransa ve İrlanda hariç 13 üye ülkede nitelikli sertifika üreticilere lisans veren bir kurum vardır. İrlanda ve İngiltere dışında 13 üye ülkede nitelikli sertifika üreticileri düzenleyen ve denetleyen bir kurum vardır. 9 üye ülkede ise ESHS'lere ilişkin yukarıda belirtilen lisanslama ve denetleme işlevleri aynı kurum tarafından yerine getirilmektedir.

5.5 ABD'de Durum

ABD Kongresi e-imza yasasını (Electronic Signatures in Global and National Commerce Act) 2000 yılında kabul etti. Bu çerçeve yasası e-imzanın uluslararası geçerliliğine değiniyor olmakla birlikte daha önce yayınlanmış olan AB Yönergesi ile tam bir uyum içerisinde olduğunu söylemek mümkün değildir.

UNCITRAL (United Nations Comission on International Trade Law) Birleşmiş Milletler bünyesinde oluşturulmuş ve uluslararası ticaret yasalarının uyumluluğunu amaçlayan bir komisyon. Çalışma alanları arasına e-ticareti de alan UNCITRAL 2001 yılında e-imza konusunda bir model yasa metni oluşturdu. Bu metin 2003 yılında Meksika ve Tayland e-imza yasaları hazırlanırken temel kaynak olarak kullanıldı.

6 Elektronik İmzanın Kullanılacağı Uygulamalar

6.1 Yapılması Gerekenler

Enformasyon teknolojileri alanındaki gelişmeler göz önüne alındığında ülkemizin büyük çaplı yatırımlar yapacağı açıktır. Bu yatırımların ekonomik yarar sağlayabilmesi ise *eşgüdümlü* ve teknolojik değişikliklere ayak uydurabilecek *esneklikte* bir planın uygulanmasıyla olasıdır. Bu amaçla devlet, birçok ülkede olduğu gibi, sanayici, kullanıcı, AR+GE, üniversite gibi bu teknolojinin ülkemizde kullanılması, benimsenmesi ve üretilmesi aşamalarında ortak çalışması gereken kurumlar arasında katalizör görevini üstlenmelidir. Bu görev aynı zamanda en büyük alıcılardan biri olan devletin (Enformasyon teknolojileri alanında bu oran en düşük olduğu ülkede dahi %10`un üzerindedir.), kendi alımları için akılcı çözümler üretmesinin de aracı olacaktır. Bu eşgüdümü sağlamak amacıyla enformasyon teknolojileri kapsamındaki tüm alanların (Cihaz ve malzeme üreticileri, Altyapı/iletişim ağı kurucuları ve işleticileri, Yazılım hizmetleri üreticileri, Hizmet sunucuları, İçerik üreticileri/sunucuları) ilgililerinin temsil edildiği bir kurumsal yapılanma en kısa zamanda oluşturmalıdır. Benzer düzenleyici kurumlar Almaya, Norveç, Danimarka, İtalya, Fransa ve İspanya gibi bir çok ülkede bakanlık olarak bulunmaktadır. Ayrı bir bakanlık çatısı altında olmasa da İngiltere, Finlandiya ve İsviçre'de düzenleyici erk enformatik alanında tek bir otoritededir. Amerika Birleşik Devletleri'nde ise düzenleyici kuruluş Kongre'ye doğrudan bağlı olarak çalışmaktadır. Bu modellerden de yararlanılarak oluşturulan düzenleyici kurum enformasyon teknolojileri alanında ki düzenlemelerde doğrudan yada dolaylı olarak taraf olan Radyo Televizyon Üst Kurulu, Telsiz İşleri Genel Müdürlüğü, Haberleşme Genel Müdürlüğü, PTT, TSE arasındaki eşgüdümü de sağlamalıdır.

Oluşturulun düzenleyici kurum kadar ülkemizin enformasyon teknolojileri alanında master planını hazırlanması da önemlidir. Master plan enformasyon teknolojilerinin gerektireceği altyapı, sunulabilecek hizmetler ve hizmetlerin sunulmasıyla değişecek ekonomik, toplumsal/kurumsal yapılanma ve düzenlemeler başlıklarını; insan kaynağı yetiştirme, teknoloji geliştirme / uyarlama, topluma yaygınlaştırabilme, uluslararası rekabet gücü olan ürünler üretebilme gibi temel sorulara da cevap üretebilecek yapabilirlik incelemelerinden geçirmelidir.

Enformasyon teknolojileri alanında incelenmesinde yarar görülen alanlar şunlardır:

- Altyapı
- Hizmetler
- Ekonomik, toplumsal, kurumsal ve yasal yapılanma

başlıkları altında, konular sıralanarak incelenmiştir.

Politika araçları alt başlığında ise değerlendirmelerin sonunda alınan kararların ülkemiz ekonomisi üzerinde olumlu etkiler yaratabilmesi için kullanılması gerekli görülen politika araçları sıralanmıştır.

6.2 Altyapı

Fiziksel altyapı değerlendirilirken, bu konunun enformasyon teknolojileri alanındaki ekonomik boyutunun büyüklüğü, sunulacak hizmetlerin çeşitliliği ve

kalitesi üzerindeki doğrudan etkisi göz önünde bulundurulmalı, hizmetleri sınırlayacak, gelişmelere kapalı çözümlerden kaçınılmalıdır.

Altyapı başlığında :

- İletişim ortamları teknolojileri (optik lif, mikro dalga, radyo frekansı vb.)
- İletişim altyapısı (erişim ve taşıyıcı şebekeler, farklı erişim ve taşıyıcı şebeke çözümleri vb.)
- Bilgi erişim ve işleme sistemleri (uç ve çevre birimler teknolojileri, yazılım geliştirme ortam ve standartları, vb.)

kapsamındaki bilgi, yetenek, donanım ve yazılım birikimimiz, bu teknolojiler kapsamında ülkemizde yapılabilecek üretimler, enformasyon teknolojilerinin ekonomik fayda yaratabilmesi için gerekecek fiziksel altyapı böylesi bir altyapının kurulmasında izlenecek politikaların oluşmasına elverecek ayrıntıda incelenmelidir. Bu incelemelerde ülkemizin bu teknolojiler kapsamında uluslararası pazarda rekabet edebilecek ürünler ortaya koyabileceği alt alanlar belirlenmesi büyük önem taşımaktadır.

6.3 Hizmetler

Enformasyon teknolojileri aracılığıyla sunulabilecek aşağıda sıralanan hizmetler ekonomik ve toplumsal faydaları, iletişim altyapısı isterleri, ne oranda ulusal katkıyla gerçekleştirilebilecekleri de göz önüne alınarak incelenmeli ve kararlaştırılan öncelik sırasına göre eyleme geçilmelidir.

6.3.1 Eğitim ve Araştırma

Eğitim ve araştırma alanı enformasyon teknolojileri kullanılmasıyla çok hızlı değişimler geçirecek alanlardır. Ülkemiz gibi genç nüfusa sahip ülke için eğitim ve araştırma alanındaki değişikliklerin önemi açıktır. İlk aşamada üç temel uygulama alanı :

- Yetişen gençliğin enformasyon teknolojisi ürünleriyle erken tanışması yoluyla uzun vadeye yönelik bir toplumsal altyapı oluşturulması,
- Eğitim-öğretim sürecinin enformasyon teknolojisi aracılığıyla ilk ve orta dereceli okullardan üniversiteye tüm aşamaların içerik olarak güncellenmesi, zenginleştirilmesi, kalitenin yaygınlaştırılması,
- Hizmet içi ve meslek dönüşüm eğitimlerinin enformasyon teknolojisi aracılığıyla yaygınlaştırılması,

incelenmelidir. Bu inceleme süreci içinde aşağıdaki sıralanan ve gelişmiş ülkelerin gündeminde olan uygulamaların Türkiye açısından değerlendirilmesi yapılmalıdır:

*** Uluslararası Elektronik Üniversiteler:** Üniversite ve yüksek okullar, bilgi teknolojilerinin bütün disiplinlerdeki eğitim, araştırma ve geliştirmede en yetkin biçimde nasıl kullanılabileceğinin ortaya konduğu odaklara dönüşmesi, yalnızca ulusal bilgi ağları ile sınırlı kalmayıp küreselleşmek ve Küresel Enformasyon Altyapısı üzerinden uluslararası dersliklerin oluşması.

*** Etkileşimli Uzaktan Eğitim:** Orta ve yüksek eğitim kurumlarında etkileşimli uzaktan eğitim vermesi aracılığıyla giderler önemli ölçüde azalması, verilen hizmetin, kaliteden ödün vermeksizin, küçük yerleşim alanlarına dek yaygınlaştırılması.

*** Kütüphanelere Erişim:** Bu altyapıyı kullanarak yerel ya da herhangi bir uzak kütüphaneye erişim, istenen bilginin taranması ve elde edilmesinde hız ve ucuzluk sağlaması.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.2 Üretim ve Ticaret

Enformasyon teknolojilerinin doğru, etkili ve bütünleşik olarak kullanılmasının üretim ve ticaret dünyasının verimini artırmadaki (işletme, pazarlama, tasarım ve üretim giderlerinin azaltmadaki), küresel bir rekabet gücü kazandırmadaki etkileri incelenmelidir. Bu inceleme süreci içinde aşağıdaki sıralanan ve gelişmiş ülkelerin gündeminde olan uygulamaların Türkiye açısından değerlendirilmesi yapılmalıdır:

- **Bilgisayar Destekli Tasarım ve Üretim**: Sanayi toplumunun bir niteliği olan büyük ölçeklerde kitlesel üretim yerini geniş bir çeşitlilik yelpazesi içinde *esnek üretime* bırakmaktadır. Esnek üretimin ürünün tariflenmesi, ürünün modellenmesi, üretim mühendisliği, üretim kontrol ve lojistik destek aşamalarında enformasyon teknolojilerinin kullanılması, üretimdeki yaygın standartlar.
- **Video-konferans:** Gerektiği an, kişilerin bulundukları yerden bağımsız olarak ve ulaşım gideri ödemeksizin iş toplantıları gerçekleşebilmesi.
- **Elektronik Ticaret:** Gerek pazar bilgileri, gerekse bu pazara sunulacak ürüne ilişkin tüm para transferleri elektronik olarak anında yapılabilmesi, örneğin pazarlamadan gelen bir bilginin, anında ne tür bir ürünün üretilmesi gerektiğini söyleyerek, bu üretim için neyin nereden ve kaça alınacağı bilgileri elde bulundurulması, gerekli satıcıların stok durumu anında bilinmesi, sipariş verilirken ilgili firmaların çalıştıkları bankalar arası para transferlerinin anında yapılması.
- **Şatış Sonrası Uzaktan Etkileşimli Eğitim:** Profesyonel ürün satan firmaların sattıkları ürüne ilişkin eğitimi müşterilere enformasyon teknolojilerini kullanarak vermesi.
- **Süper Bilgisayar Ağları ile Bağlantı:** Süper bilgisayarlar gibi büyük yatırımların küçük işletmeler tarafından ortak satın alınması, kullanılması.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.3 Kamu Hizmetleri

Bilgi Teknolojilerinin kamu yönetiminde kullanımının kamu hizmetlerinin kalitesi, maliyeti, böylesi bir sistemin getireceği dolaysız ve açık kamu birey ilişkilerini etkileri incelenmelidir. Bu inceleme süreci içinde aşağıdaki sıralanan ve gelişmiş ülkelerin gündeminde olan uygulamaların Türkiye açısından değerlendirilmesi yapılmalıdır:

- **Elekronik Belgeler:** Bireylerin devletten almak zorunda olduğu ve devletin tuttuğu diğer kayıtlarda (nüfus kağıdı, pasaport, tapu ve kadastro, nüfus, adli kayıt ve sicil, askerlik, ithalat/ihracat vb.) enformasyon teknolojilerinin kullanılması.
- **Ödemeler:** Vergi, harç v.b. ödemelerin enformasyon altyapısı üzerinden yapılması.

- **Veri Aktarımı:** Devlet içi yazışmaların, belge ve veri aktarımların, enformasyon altyapısı üzerinden sağlanması.
- **Video-konferans:** Kamu görevlilerinin toplantılarında zaman ve mekandan bağımsız enformasyon altyapısı üzerinden yapılması.
- **Elektronik Oylama:** Elektronik oylama ya da referandum ile bireylerin yönetime katılımı etkinleştirilerek daha çoğulcu bir demokratik düzene geçilmesi.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.4 Sağlık Hizmetleri

Enformasyon altyapısı sağlık hizmetlerinde kullanılmasının sağlık hizmetlerinin kalitesi, kalitenin yaygınlaştırılması ve hizmetlerin maliyetleri üzerindeki etkiler incelenmelidir. Bu inceleme süreci içinde aşağıdaki sıralanan ve gelişmiş ülkelerin gündeminde olan uygulamaların Türkiye açısından değerlendirilmesi yapılmalıdır:

- **Uzaktan Tarama:** Röntgen, ultrason, tomografi gibi sağlık taramalarının her hangi bir yerde yapılıp uzaktaki bir uzman hekimin incelemesine enformasyon altyapısı üzerinden sunulması.
- **Video-konsültasyon:** Her hangi bir yerdeki hastaya, bulunduğu yerden bağımsız olarak uzmanların enformasyon altyapısı aracılığıyla uzaktan konsültasyon yapması.
- **Sağlıkla İlgili Veri Bankaları:** Bireylerin sağlıkları ile ilgili tüm verileri düzenli bir biçimde veri bankalarında saklanması.
- **Koruyucu Sağlık Hizmetlerinin Uzaktan Sunulması:** Bireylerin koruyucu sağlık hizmetlerini evlerinde enformasyon altyapısı üzerinden akıllı terminaller aracılığıyla yapabilmesi.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.5 Yasama ve Yargıya Yönelik Hizmetler

Enformasyon teknolojilerinin yasal düzenlemelerde demokrasinin yaygınlaştırılması ve yasama ve yargının hızlı ve güvenilir çalışmasına yönelik uygulamaları incelenmelidir. Bu amaçla başlangıç olarak aşağıdaki projeler değerlendirilebilir:

- **Hukuk Düzeninin Çelişkilerden Arındırılması:** Enformasyon teknolojilerinin kullanımıyla hukuk düzeninin yeniden gözden geçirilmesi, çelişkili uygulamaların ortadan kaldırılmasında kullanılması.
- **Bireyin Parlementoya Katılımı:** Bireylerin parlementodaki çalışmaları yakından izleyebilmesi, çıkartılmakta olan yasalar hakkında daha geniş bilgi sahibi olabilmesi.
- **Bireyin Yasal Uygulamaya Etkin Katılımı:** Bireyin kendisi ile ilgili yasal verilere erişebilmesi, durumunu (örneğin her hangi bir yasaya olan karşı davranışı gibi) tüm açıklığı ile görebilmesi, bir suç oluşmadan gereken önlemleri ve düzeltmeleri uygulmasına yönelik hizmetler.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.6 Evlere Hizmet

Bilgi teknolojileri, bireyin evinden çıkmadan pek çok gereksinimini sağlamasına olanak tanımaktadır. Sunulacak evden çıkmadan alışveriş, çeşitli ödemeler yapma olanakları getirecekleri sosyal etkilerde göz önünde bulundurularak ekonomik yönden incelenmelidir. Bu incelemeye başlangıç noktası olarak aşağıdaki sıralanan ve gelişmiş ülkelerin gündeminde olan uygulamaların Türkiye açısından değerlendirilmesi yapılmalıdır:

- **Evde Çalışma (tele-iş):** Bireylerin işe gidip gelmek için harcadıkları zamanı azaltacak, çalışma ortamının ev olmasını sağlayacak uygulamalar.
- **Güvenlik Hizmetleri ve Sayaçların Uzaktan Okunması (telemetre):** Elektrik, su, gaz v.b. idareler bireyin konutuna gelmeden sayaçları okuması ve bu şebekelerdeki güvenliğin, hizmetin sürekliliğinin enformasyon teknolojileri aracılığıyla denetlenmesi.
- **Evden Alışveriş ve Banka Hizmetleri:** Etkileşimli çoklu-ortam ve sanal gerçeklik uygulamaları yardımıyla insanların alacakları giysileri üzerlerinde nasıl duracağına bakması, ev eşyalarının yerlerini değiştirmesi vb., alış veriş sonucunda ücreti elektronik olarak ödemesi.
- **Bilgi Alma Hizmetleri:** Bireylerin yasa, yönetmelik vb. konularda güncel bilgilere ulaşabilmesi, coğrafi bilgi sistemlerine erişim kolaylıkları, sanat, spor, ulaşım alanlarında rezervasyon vb hizmetlere ulaşabilme.
- **Video Postası ve Video Telefon:** Görüntülü posta ve telefon hizmetlerinin enformasyon altyapısı aracılığıyla sunulması.
- **Ismarlama Video (video on demand):** Bireyin evinde ayrı bir video göstericisi ve video kaset koleksiyonu olmadan, evindeki uç biriminden merkezi bir bilgi bankasına erişerek dilediği video filmini izleyebilmesi, gerektiğinde durdurup geri sardırabilmesi.
- **Etkileşimli Çoklu Ortam ve Video Oyunları:** Bireyin eğlenme isteklerine yeni ve yaratıcı çözümler sunabilecek etkileşimli, yaratıcılık yeteneği kazandıran oyunların enformasyon altyapısı aracılığıyla sunulması.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.3.7 Topluma Yönelik Diğer İletişim ve Bilgi Hizmetleri

Toplumun kolay, güvenilir ve doğru bilgilendirilmesini sağlayacak uygulamalar yaratacağı önemli sosyal değişiklikler de göz önünde alınarak değerlendirilmelidir. Bu değerlendirmelerin başlangıç noktası olarak da aşağıdaki uygulamalar önerilebilir :

- **Elektronik Gazete ve Kaynak Bilgiler:** Elektronik gazete ve kaynak bilgilerin derli bir biçimde sunulması, aranılan bilgiye erişimi kolaylaşması.
- **Toplumu İlgilendiren Bilgi Hizmetleri:** Toplumu ilgilendiren zamanında bireylere ulaşması.
- **Elektronik Duyuru Hizmetleri:** Enformasyon Altyapısı ivedi duyuruların topluma anında iletilmesini için kullanılması.

- **Hizmetleri Tanıtan Rehberler ve Sınıflandırılmış Reklamlar:** Bilgileri ve hizmetleri tanıtan, sınıflandıran sistemlerin kullanılması.
- **Elektronik Müzeler ve Kütüphaneler:** Elektronik Müzeler ve Kütüphaneler, bireyin yaşadığı çevre ve kültür birikimi ile yakınlaşmasını sağlamansına yönelik uygulamamalar.

Bu değerlendirme sonucunda böyle bir programın başlatılması için kaynakların kullanımı, eylem planı ve gerek yeni istihdam olanakları gerekse ulusal gelire katkısını irdeleyen ekonomik yararları ortaya konulmalıdır.

6.4 Toplumsal/Kurumsal/Yasal Yapı ve Düzenlemeler

Jenerik teknolojilerden ve bunların başında gelen enformasyon teknolojisinden beklenen ekonomik yararının sağlanabilmesi için, bu teknolojilerin, ilintili bulundukları bütün ekonomik etkinlik (aktivite) alanlarına yayınması (difüzyonlarının sağlanması) gerekir. Aslında, yukarıda işaret edilen, "üretim sisteminin yeni jenerik teknolojiler tabanında yeniden biçimlenmesi" söz konusu teknolojilerin bütün üretim alanlarına yayınmasını ve bu teknolojilerden tam anlamıyla yararlanır hale gelmeyi; özgül kullanım alanlarına göre, ürün bazında olsun, üretim yöntemi bazında olsun, bunları uyarlama ve geliştirme yeteneğinin kazanılmasını içerir.

Bellidir ki, bu sürecin başarısı bu yayınmayı mümkün kılacak toplumsal/kurumsal düzenlemeleri gerektirir. Eğitim, öğretim ve AR+GE sisteminde; AR+GE'nin finansman ve teşvikinde; vergi sisteminde; mali mevzuatta; konu ile ilgili hukuk sistem ve mevzuatında; devletin satın alma politikasında; devletin "regülasyon" alan ve kurallarında; akreditasyon-sertifikalandırma kural ve sistemlerinde; kalite ve standartlar konusuna ilişkin kural ve mevzuatta; çalışma hayatının, işçi-işveren ilişkilerini konu alan mevzuat ve kurumsal yapılanmalarda ve buna benzer pek çok alanda uygun düzenlemeler yapılmaksızın jenerik teknolojilerin yayılmasını ve yayınmasını, dolayısıyla de bunlardan beklenen ekonomik yararı sağlayabilmek mümkün değildir. Dahası, yeni jenerik teknolojilerin, temelde, yeni bir yaşama biçim ve kültürünü tanımladığı; bunun geleneksel yapılarda bazı sıkıntılara yol açabileceği; hatta, gerekli toplumsal önlemler alınmazsa, işsizlik gibi son derece önemli sorunlarla karşılaşabileceği asla göz ardı edilmemelidir. Teknoloji mükemmel bir araçtır; ama son çözümlemede onu kullanacak olan insandır. Teknolojiyi kullanacak insan, o teknolojiyle barışık olmalıdır. Bunun için de onun bilgi ve kültürünü edinmiş; yaşam alanları ve bu alanlarla ilintili toplumsal kurumlar o teknolojinin gerekleriyle uyumlu hale getirilmiş olmalıdır.

Aşağıda enformatik alanında yapılacak atılımdan beklenen yararın sağlanabilmesine yönelik ilk aşamada yapılması gereken yasal/toplumsal/kurumsal düzenlemelere işaret edilmiştir. Bu konularda son derece ciddi çalışmaların bir an önce başlatılması önemlidir.

6.5 Yasal Düzenlemeler

Yasalar, toplumsal yaşamı düzenlemek için çıkarılır. Toplum eğer bir devrim geçiriyorsa, yasal düzenlemelerin de yeniden gözden geçirilmesi gerekmektedir. Örneğin Sanayi Toplumunda, daha önce var olamayan, sendikal haklar, grev / lokavt, trafik v.b. pek çok yeni kavrama ilişkin yasalar çıkarılmıştı. Dahası, telif haklarını ihlal

gibi daha önce bilinmeyen suçları da tanımlanmak gerekmişti. Sanayi Toplumuna göre çok daha karmaşık bir yapısı olacak olan gelecek yüzyılın toplumunda, doğal olarak çok karmaşık sorunların düzen altına alınabileceği yasal düzenlemeler gerekecektir. Bunların bir bölümünü aşağıdaki gibi özetleyebiliriz:

Enformasyon Teknolojilerinin kullanımını engelleyecek ya da karmaşıklaştıracak gereksiz tüm mevzuat (elektronik iletilerin yasallık kazanması, bilgilerin elektronik olarak korunması,kodlanması ile ilgili düzenlemeler, sayısal imzanın yasallık kazanması vb.) yeniden gözden geçirilmelidir.

Kağıt ortamda basılı yapıtların korunması için çıkarılmış olan telif hakları köklü bir değişiklikten geçmelidir. Bu, yalnızca geliştirilen uygulama yazılımlarını da koruma altına almak gibi dar açıdan ele alınmamalı, örneğin, çoklu ortamda geliştirilen v.b. ürünlerin kullanıcılarca değiştirilip yeni bir ürün olarak Enformasyon Altyapısına sunulma durumlarını da içerecek biçimde çok yönlü olarak ele alınmalıdır.

Sanayi ürünleri genelde bir ya da bir kaç kişinin ortak çalışması ile ortaya çıkan ve göreli olarak basit ürünlerdi. Oysa Sanayi Ötesi Toplumun ürünleri, ancak belli bir birikimin sonucu ekip çalışması ile ortaya çıkarılabilmektedir. Bu çalışmada yalnızca bireylerin değil, firmaların da birikimi, başka bir deyişle entellektüel varlıkları kullanılmaktadır. Bu durum, telif haklarından çok değişik yeni bir kavramın, düşünce iyeliği hakkının (*Intellectual Property Rights*) tanımlanmasını ve korunmasını getirmektedir.

Kısacası, bugün dayandığımız yasal mevzuat orijinal kopya, ıslak imza gibi anlamını yitirmiş ve teknolojik gelişmelere gözünü kapatmış bir ortamdadır. Enformasyon Altyapısının dayandığı sayısal teknolojiye (*digital technology*) ayak uydurabilen bir yasal düzenlemelere doğru bir geçiş kaçınılmaz olduğundan ayrıntılı olarak incelenmelidir.

6.5.1 Mahremiyet

Enformasyon teknolojilerinin kullanımıyla topluma ve bireylere ilişkin her tür bilginin bu ağda şu ya da bu biçimde saklanacağı görülmektedir. Birey ya da kuruluşlar, kendi olurları alınmadan kendilerine özel bilgilerin bu ağa aktarılmasına izin vermeyeceklerdir. Dolayısı ile kişi ya da kuruluşlara ilişkin mahremiyet ya da kişisel gizlilik (*privacy*) sağlanmadığı sürece enformasyon altyapısı verimli olarak kullanılamaz. Gizliliğin tanımı enformasyon teknolojilerinin kullanımı dikkate alınarak yeniden tanımlanmalı, ihlali ile ilgili yasal yaptırımlar yeniden düzenlenmelidir.

6.5.2 Sınır Ötesi Veri Aktarımı

Enformasyon teknolojilerinin yaygın kullanılması ile sınır ötesi veri aktarımı (*Transborder Data Flow*) ile ilgili sorunlar daha da güncel hale gelecektir. Ülkeler arasındaki hukuki farklılıklardan kaynaklanan yeni suç çeşitleri ve bunlara karşı uygulamalar dünyada tartışılmaktadır. Ülkemiz taraf olduğu uluslararası anlaşmalardan kaynaklanan yükümlülüklerini yerine getirmek için önlemler alması gereken bu konuyu da incelemelidir.

6.6 Politika Araçları

Enformasyon teknolojilerinin ülkemizde yaygınlaşması, özümsenmesi ve geliştirilebilir, üretilebilir hale gelmesinde, altyapı, hizmetler yada toplumsal/ekonomik/kurumsal yapılanma alanında alınan kararların olumlu ekonomik etkilerinin hızlı görülebilmesi için aşağıdaki araçlardan yararlanılabilir. Bu araçlar enformasyon teknolojileri hizmetleri alanında yapılabilirlik incelemeleri olumsuz çıkan, ancak stratejik önem taşıyan alanlardaki eksikliklerin giderilmesinde de önemli rol oynayacaklardır.

- Devletin özendirici ve düzenleyici politika araçları
- **Siyasal baskılardan etkilenmeyecek kadar kararlı, teknolojik değişikliklere ayak uydurabilecek kadar esnek bir devlet satın alma politikası belirlemek:** Bütün ileri sanayi ülkelerinin ve yeni sanayileşen ülkelerin, sanayileşme eşiğini aşıncaya dek kullana geldikleri ve bugün de, ekonomilerini geliştirmek ve rekabet üstünlüklerini sürdürmek için kullanmakta oldukları bu araçtan, Türkiye'de de, *enformasyon teknolojisi üreticisi ülke* olmak amacıyla yararlanılmalıdır. Böyle bir satın alma politikası devletin alımlarında yerli üretici/girişimci ve AR+GE kurumlarının önünü açıcı olmalı, yerli üretici ve girişimcilere hazırlıkları için makûl süreleri sağlamalıdır.
- **Enformasyon teknolojileri alanının kapsamındaki mal ve hizmet standartları belirlemek, kamu kurumları için standardizasyonu daha katı kurallarla uygulamak:** Ulusal ve uluslararası pazarda üretici ve akıllı bir tüketici olmak uluslararararası standartların yerleştirilmesi, yaygınlaştırılmasıyla mümkündür. Enformatik alanı, içerdiği geniş mal ve hizmetlerin çeşitliliğiyle, standartlar konusunda hata ve eksiklikler yapılırsa, teknoloji çöplüklerine ve uyumsuz ortamlara dönüşebilir. Kamu kurumları bu standartlara en katı şekilde uyması gereken kurumlardır. Bu konuda yapılmış çalışmalar hızla uygulamaya konulmalıdır.
- **Mal ve hizmet standartlarının belirlendiği uluslararası platformlarda etkin temsil edilmek:** Enformatik alan kapsamındaki mal ve hizmetlerin standartlarının belirlendiği platformlarda karar alma süreçlerine etkin olarak katılmak, bu ürün ve hizmetlerin ülkemizde tüketilmesi ve üretilmesi ortamlarını doğrudan etkileyecektir. Türkiye yazıcılar ve klavyeler alanında yaşadığı kötü pratiği göz ardı etmemelidir.
- **Yazılı ortamda da kısıtlı olan veri bankalarının zenginleştirilmesini, elektronik ortama geçirilmesini özendiren/zorunlu kılan düzenlemeler yapmak:** Kurulacak bir ulusal enformasyon şebekesinden ekonomik yarar elde edebilmek, bu şebekede dolaşacak ulusal kaynaklı verilerin elektronik ortamda varlığına bağlıdır. Ulusal AR+GE ve üretim faaliyetlerine kaynaklık edecek verilerin, yayınların, kütüphanelerin enformasyon teknolojisi aracılığıyla geniş kitlelerin erişime açılması hedeflenmelidir.
- **Enformasyon teknolojileri alanında yetkin özerk düzenleyici kuruluş (regulatory body) oluşturmak:** Enformasyon teknolojileri alanının yapısından kaynaklanan genişliği kavrayacak, çok başlılığı önleyecek düzenleyici kuruluşun yokluğu önemli bir eksikliktir. Bu alanda diğer ülkelerde örnekleri olan, Meclise, Hükümete yada bir Bakanlığa karşı sorumlu özerk bir kurum modeli seçilmeli, halen enformatik alanında var olan düzenleyici yada ilgili kurumlar arasında (Radyo Televizyon Üst Kurulu, Telsiz Genel Müdürlüğü, Haberleşme Genel Müdürlüğü gibi) koordinasyonu sağlamalıdır.
- **Üretim sistemlerinde enformasyon teknolojilerinin kullanımını özendirmek:** Üretim sistemlerinde teknolojik tabanın değişimine ayak uydurmak ülkemizin rekabet gücü olduğu üretim alanlarında bu gücünü korumak, yeni alanlarda rekabet gücü kazanmak için önemli bir gerekliliktir. Üretimin teknolojik tabanının esnek üretim/esnek otomasyon, yeni iş/yeni organizasyon ("labor process") temelinde değişmesi desteklenmelidir. (Uzun vadeli teknoloji dönüşüm kredileri vb.)

- Eğitim ve araştırma-geliştirmeye yönelik politika araçları
- **Doktora, yüksek lisans, lisans, ön lisans ve meslek lisesi seviyesinde enformatik alanına yönelik insan gücü yetiştirmek**: Enformasyon teknolojileri mal ve hizmetlerinin düşünceden ürüne dönüşme süreci, diğer sanayi üretimiyle karşılaştırırlığında çok daha kısadır. Bu sürecin kısalığı enformatik alanında bilim üretiminin önemini bir kat daha artırmaktadır. Üniversitelerde enformatik alanında doktora, yüksek lisans ve lisans programlarına önem verilmelidir. Enformasyon teknolojilerinin toplumda yaygınlaşması ve kullanılabilmesi ön lisans ve meslek lisesi seviyesinde yetişmiş insan gücüyle mümkün olacaktır.
- **Eğitim sistemininde enformasyon teknolojilerini kullanmak:** Eğitim sisteminde enformasyon teknolojilerinin kullanılmasının genç nüfusun eğitim gereksinimini kaliteden ödün vermeden karşılanmasında önemli rolü olacaktır. Eğitim sisteminde enformasyon teknolojilerinin kullanılması, bu teknolojilerin toplumda kabul görmesi için gerekli ortamın hazırlanmasında payı büyük olacaktır.
- **Enformasyon teknolojileri alanında araştırma geliştirmeyi desteklemek:** Enformasyon teknolojileri mal ve hizmet üretimleri ülkemizde gerçekleştirmenin yolu araştırma geliştirme faaliyetlerinden geçmektedir. Yoğun olarak entellektüel faaliyete dayanan enformasyon teknolojileri mal ve hizmetlerinin üretilebilmesi için, üniversite-sanayi işbirliği, kamu ve özel kesimin ortak araştırmaları, enformatik alanının sosyal etkilerinin inceleneceği disiplinler arası ortak araştırmaları, girişimciliğin ve yaratıcılığın özendirilmesini sağlayacak enformatik alanına yönelik teknoparkların kurulmasını öncelikli olarak kullanılması gereken politika araçlarının başında sayabiliriz.
- Enformasyon teknolojilerinin kullanımının kabul görmesi ve yaygınlaşmasına yönelik politikalar
- **Kamu pilot projeleri**: Kamu kesimi kendi işleyişini yeniden düzenlemek amacıyla var olan enformasyon teknolojisi birikimini kullanılmaya başlamalı, bu yönde personel altyapısı oluşturmalıdır. Eğitim kurumlarında, sağlık ve sosyal yardım kurumlarında ve vergi dairelerinde başlatılacak pilot projeler toplumun enformatik alanıyla olan yakınlığı artırmanın yanı sıra üretici olmak isteyen girişimciler için de ortam yaratacaktır.
- **Özel sektör pilot projeleri:** Özel sektörün enformasyon teknolojileri alanında geliştirdiği/ürettiği yeni mal ve hizmetlerin gösterimlerini yapılabileceği gösterim merkezleri kurulmalı ve bu merkezlerdeki gösterimler desteklenmelidir.

7 Elektronik İmza ve Uluslararası Geçerliliği

Elektronik sertifikaların, yayınlandığı ESHS kapsamı içerisinde kullanılması ile beraber diğer ulusal ve yabancı ESHS'ler ile de çalışabilmesi gerekmektedir. Faktör, bilginin gizliliği, bütünlüğü, iki tarafta da kimlik belirleme, zaman kavramının sabitlemesi, Ulusal ve Uluslararası Kanun/Mevzuat ihtilaflarının giderilmesi için elektronik kayıtların ihtilaflarda ispat gücünün ihtilafsız kabulü, uç kullanıcıya kadar güvenli altyapı gibi temel işlemler için Ulusal bazda Hukuki Altyapı, İdari, Teknik ve Uluslararası altyapının kurulması gerekir. ESHS'lerin karşılıklı çalışabilirliği sağlanırsa, Elektronik Sertifikaların Uluslararası kullanımı mümkün olacaktır. Teknik özellikler, ilkeler, iş ilişkileri ve yasal değerlendirmeler de gözönüne alınarak ESHS'ler arasında karşılıklı çalışabilirliği sağlamak üzere önerilmiş ve geliştirilmiş birçok metod vardır. Bu metodlar Dünyanın çeşitli ülkelerinde ortak çalışmalarla test edilmekte ve uygulanmaktadır. Henüz çok kesin ve net standartlar ortaya konulmamış olsa da bu metotlardan bazıları ön plana çıkmayı başarmıştır. Bu çalışmada, önerilmiş ve bazıları

uygulanmakta olan metodlar avantaj ve dezavantajları gözönüne alınarak incelenmiştir.

7.1 ESHS'ler Arası Karşılıklı Çalışabilirliğin Gerekliliği

ESHS'ler arasında teknik, ilke, iş ve yasal bakımdan farklılıklar bulunabilmesinden dolayı karşılıklı çalışabilirlik, üzerinde özenle durulması gereken bir konudur. Bir ESHS'nin kendi sınırları içerisinde hizmet vermesi ile birlikte, diğer ulusal ESHS'ler ve uluslararası ESHS'ler ile de karşılıklı olarak belirlenmiş güven ilişkileri içerisinde çalışabilmesi gerekir. Ülkelerarası ve farklı AAA etki alanları arasında karşılıklı çalışabilirliği sunmak amacıyla, standartlaşma sağlamak üzere birçok çalışma devam etmektedir.

Karşılıklı çalışabilirlik, bir ESHS tarafından yayınlanan Elektronik Sertifikaların, yurt içindeki ve yurt dışındaki güven duyabileceği başka ESHS'ler ile de sorunsuz olarak iletişim ve güven ilişkileri kurabilmesi yeteneğidir. Karşılıklı çalışabilirliği sağlamak üzere önerilen seçenekler arasından seçim yapmak üzere aşağıdaki üç ana alan üzerinde belirginlik sağlanmalıdır (Lloyd, 2001):

- Karşılıklı anlaşma düzeyine bağlı olarak karşılıklı çalışabilirliği kolaylaştırmaya yardımcı olacak protokol, veri yapısı, sertifika ilkeleri, sertifika uygulama esasları, sertifika ve sertifika iptal listelerinin paylaşılması gibi teknik değerlendirmelerin göz önüne alınmasıdır.
- Karşılıklı ilkeler ve iş ilişkileri ile ilgili konuların değerlendirilmesidir. Bu alan, ESHS'ler arasındaki ilişkileri tesis etmek üzere, teknik olmayan detayları kapsar. Kuruluşlar arası ilişkilerin elektronik bilgi alışverişine dayanacak şekilde kurulması mantığıdır. Bu "elektronik ilişki", mevcut gereksinimlerden dolayı bir veya birden fazla uygulamaya bağlı olarak bilgi alışverişinde bulunmak üzere gerçekleştirilebilirken, zamanla ortaya çıkabilecek gereksinimleri de içerebilir. Kısacası, yabancı bir ESHS tarafından çıkarılan sertifikaların yerel ESHS'da ve yerel ESHS tarafından çıkarılan sertifikaların yabancı ESHS'da nasıl kullanılacağını açıklar.
- Bu alanda ise, yasal değerlendirmeler göz önüne alınır. Karşılıklı çalışabilirlik konusunda karşılaşılabilecek en önemli sorun, farklı hukuki altyapılara sahip ortamlardır. Bu kapsamda ESHS'ye ve kullanıcıya düşen sorumluluk ve yükümlülüklerin iyi anlaşılması gerekir. Buna, göz önüne alınması gereken "Yasal bildirimler ne içerecek ve bu bildirimler güvenen tarafa nasıl taşınacak?" gibi kullanıcı bilgilendirme gereksiniminin kapsadığı yükümlülükler örnek olarak verilebilir.

7.1.1 Hukuki Altyapı

Elektronik imza ile ilgili hukuki altyapının oluşturulması ile ilgili şu çalışmalar gerçekleştirilmiştir:

- Her türlü ikili ve kurumsal iş ve işlemlerde kayıt tutma, standart ve tekniklerinin belirlenmesi,
- Elektronik kayıtların kamu kurum ve kuruluşları tarafından belge olarak kabulü ile ilgili standart ve iç mevzuatlarının düzenlenmesi,
- Ticaret Kanunu, Sayıştay denetim usulleri, Borçlar Kanunu, Bankalar ve Vergi Usul kanunlarının elektronik belge tutma ve gönderme şartları göz önüne alınarak tekrardan düzenlenmesi,
- Elektronik ortamda oluşturulan yabancı belgelerin geçerliliği konusunda Dış Ticaret, Gümrük ve Bankalar Kanununda değişiklik, Uluslararası/Ulusal olarak

yapılan Elektronik Sözleşmelerde ve sanal ticarette oluşabilecek ihtilaflar konusunda Elektronik Tahkim Yasasının çıkarılması,

- Özel ve kurumsal bilgilerin gizliliği, bütünlüğü için Ulusal Bilgi Güvenliği Yasasının çıkarılması buna bağlı olarak SPK gibi kurumların ve ürün borsalarında kontrat bazlı, spot ve opsion piyasalarında sanal işlem uygulama yönetmelikleri ile Uluslararası sanal ticaret için akreditasyon kurumları için yeni mevzuatların çıkarılması,
- Açık anahtar (public key) ile ilgili onay kurumlarının (Nitelikli Elektronik Sertifika sağlayan kurumların) kurulum izinleri ve denetimi kamu tarafından yapılmalı, %51 hissesi kamu elinde bulunan kurumların bu pazardan ivedi çekilmesi gerekmektedir, Uluslararası kredi ve finans kurumlarının ticarette uyguladığı kriterlerin devlet kurumlarının hizmet ve mal alımında da uygulanması için Devlet İhale Kanunu, Elektronik İmza Kanunu ile Elektronik İmza Yönetmeliği'ne kesin ve bağlayıcı maddelerin ilave edilmesi,
- Elektronik suçların evrenselliği konusunda yapılan uluslar arası mevzuat çalışmaları ve yapılacak ikili anlaşmaların hızlı bir şekilde yapılması, işlerlik açısında delil toplama ve alma/verme standartlarının belirlenmesi.
- Elektronik Kontrat ve Elektronik İmza gerektiren sanal işlemlerde Tüketicinin Korunması ile ilgili mevzuatın elektronik ticaret açısından yeniden gözden geçirilmesi, e-trade yapan kurumların uyacağı kuralların ivedilikle yayınlanması, Bankacılık kanunu ile ilişkilendirilmeli ve charge-back sisteminin sanal ticarette uygulamaya sokulması,
- Elektronik ödeme araçları arasında yer alan elektronik paranın (elektronik senet, elektronik çek, elektronik teminat, gibi) uygulanacağı standart, teknikler ve güvenlik kriterleri ile ulusal ve uluslar arası dolaşımı mevzuat ve anlaşmaların yapılması,
- Elektronik imza yasası,
- Elektronik imza ile ilgili yönetmelik,
- Elektronik arşivle ilgili yasal mevzuat,

7.1.2 İdari Altyapı

Elektronik İmza Yasası ile idari sorumlu tamamen Türk Telekomünikasyon Üst Kurumu olarak tayin edilmiştir. Yönetmelik gereği Nitelikli sertifika sağlayıcı kurumların lisans işlemlerinden tutun uygulamadaki kurallara kadar hazırlanmış bulunmaktadır. Uluslararası bilgi değişim modülü ve anlaşmalar konusunda Adalet Bakanlığı, Dış Ticaret Müsteşarlığı, Gümrük Müsteşarlığı ve Bankalar Birliği ile ortak çalışma başlatması beklenilmektedir.

Elektronik Arşiv konusu ve veri değişim standartları konusunda Başbakanlık Arşivler Genel Müdürlüğü ilgili mevzuatı çıkarmış ve bundan sonra kurumların yazışma ve değişim modüllerinde uyacağı kurallar belirlenmiştir.

Tüm kamu kurum ve kuruluşlarında ivedi olarak iş yapış tekniklerini ve uygulamaya dönük mevzuat çalışmasını ulusal ve uluslararası e-imza normlarına göre tekrar düzenleyip yayımlaması gerekmektedir.

7.1.3 Teknik Altyapı

ESHS'lerin yayınladığı Nitelikli Elektronik Sertifikalar'ın uluslararası çapta da geçerliliğine ihtiyaç olabilir. Bu amaçla, ulusal ve uluslararası çapta birlikte

çalışabilirliği ve uyumluluğu sağlamak üzere önerilmiş ve geliştirilmiş birçok metod vardır. ESHS'ler arası karşılıklı çalışabilirlik, herhangi bir yöntemle ESHS'ler arasında kurulan güven ilişkisine dayanır. Çeşitli uluslararası ESHS'lar tarafından kullanılmakta ve/veya test edilmekte olan bazı metodlar aşağıda sıralanmıştır:

- Çapraz-Sertifikasyon
- Köprü ESHS
- Çapraz-Tanıma
- Sertifika Güven Listeleri
- Akreditasyon Sertifikası
- Mutlak Hiyerarşi
- Yetkilendirilmiş Yol Onaylama ve Bulma

Karşılıklı çalışabilirlik için AAA'lar ve ESHS'ler tarafından gerçekleştirme biçimine ve düzeyine bağlı olarak bu önerilerden biri veya birkaç tanesi kullanılabilmektedir. Oluşturulmak istenen güven ilişkileri sağlanırken, belirli durumlarda ortaya çıkabilecek riskleri hafifletmek ve farklı türdeki problemleri gidermek üzere seçenekler arasından tercihler yapılabilir. Hangi güven formunun seçileceği genellikle kuruluş politikaları ile belirlenir (Entrust, 2000).

7.1.3.1 Çapraz Sertifikasyon

Çapraz-sertifika, bir ESHS tarafından başka bir ESHS'ya, karşıdaki ESHS'nin genel anahtarını içerecek şekilde dijital olarak imzalayıp yayınladığı genel anahtar sertifikasıdır (Kiran, 2002). Temel olarak bir ESHS kullanıcılarının, kendi ESHS'leri ile çapraz-sertifikalandırılmış diğer ESHS kullanıcılarına güven duymasıdır (Entrust, 2000). ESHS'ler arasında Çapraz-Sertifikasyon gerçekleştirilirken çalışma ilkeleri, birbirlerine duyacakları güven düzeyi (tamamen eş-düzeyli veya belirledikleri güven düzeyleri arasında eşleştirme biçiminde olabilir) ve teknik bağlantılarla ilgili karşılıklı uzlaşmaya varmış olmaları gerekir (Entrust, 2003).

Çapraz-Sertifikasyon terimi ile kastedilen iki işlem biçimi vardır (Turnbull, 2000)

Genellikle seyrek olarak gerçekleştirilen ilk işlem biçimi, iki ESHS arasında "Çapraz-Sertifika" diye adlandırılan bir sertifikada diğer ESHS'nın genel anahtarının imzalanması ile ESHS'lar arasında güven ilişkisinin kurulmasıdır.

İstemci uygulaması tarafından sıklıkla kullanılmakta olan diğer işlem biçimi ise, AAA ağı içerisinde bir ESHS tarafından imzalanan kullanıcı sertifikasının güvenilirliğinin onaylanmasını gerektirir.

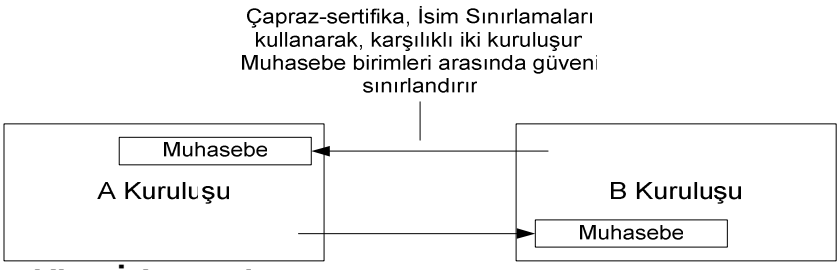
Ölçekleme nedenleriyle birden çok ESHS gerçekleştiren kuruluşlar için çapraz sertifikalandırılmış ESHS'ların kendi aralarında tam güven ilişkisi uygun olabilir. Ancak, belirli ve sınırlı iş ilişkilerine sahip farklı kuruluşlar için ESHS'ler arasında tam güven ilişkisinin kurulması genellikle uygun olmaz. Bu yüzden güven ilişkilerinin sınırlandırılması gerekmektedir.

Çapraz-Sertifikasyonda karşılaşılan diğer eleştirilerden birisi de, birden çok ESHS boyunca "Geçişli Güven" diye de adlandırılan, istenmeyen güven zincirleri ortaya çıkarabilmesidir. Örneğin ESHS1, ESHS2'ye güveniyor ve ESHS2'de ESHS3'e güveniyorsa, ESHS1'in ESHS3'e güveniyor olmasını önlemek gerekebilir. Çapraz-Sertifikalarda bu güven zincirini önlemek ve güven ilişkilerini sınırlandırmak üzere

geliştirilmiş bazı eklentiler mevcuttur. Bunlar: İsim Sınırlamaları, İlke Sınırlamaları ve Yol Uzunluğu Sınırlamalarıdır.

7.1.3.1.1 İsim Sınırlamaları

İsim sınırlamaları, çapraz-sertifikalandırılmış ESHS'ler arasındaki güven ilişkisinin, ayırt edici isim ile belirli nesne alt grubu veya gruplarına sınırlandırılması için kullanılmaktadır (Turnbull, 2000). Örneğin, A kuruluşunda çalışanların alt kuruluş birimleri şeklinde organize edildiğini ve muhasebe birimindeki kullanıcıların '*cn=Ahmet Ozturk, ou=Muhasebe, o=A, c=TR*' şeklinde, satış birimindekilerin de '*cn=Serap Ozdemir, ou=Satis, o=A, c=TR*' biçiminde olduğunu varsayalım. B kuruluşunda da böyle bir yapılandırma varsa, A ve B kuruluşları için sadece muhasebe birimlerindeki kullanıcılar arasında sınırlandırılmış bir güven ilişkisi oluşturulabilir (Şekil 16).



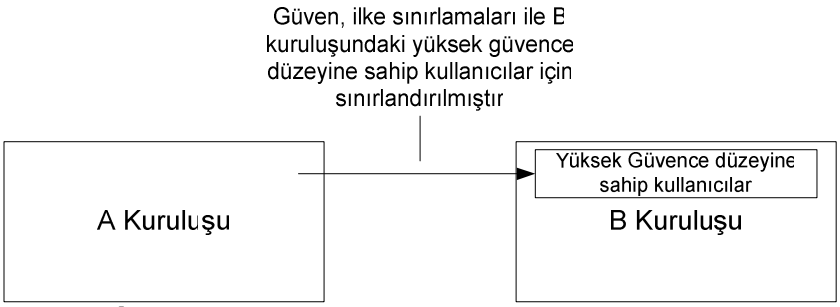
Şekil 16 İsim Sınırlaması

7.1.3.1.2 İlke Sınırlamaları

İlke sınırlamaları, çıkarılan sertifikaların yabancı AAA etki alanındaki belirli ilke değerlerine sahip nesnelerle güven ilişkisi kuracak şekilde kullanımını sınırlamak üzere kullanılabilmektedir (Turnbull, 2000).

İlke sınırlamalarına örnek olarak, kullanıcı güvence düzeyleri verilebilir. Güvence ile kastedilen, sertifikada belirtilen kişinin gerçekten o kişi olup olmadığından emin olma derecesidir. Organizasyonlar, kullanıcısına sertifikasını çıkarmadan önce kullanıcıyı doğrulamak üzere kullanılan yöntem için farklı düzeyler kullanabilirler. Düşük güvence gerektiren bir ilke için telefonla, etkinleştirme kodu istenmesi yeterli olabilecekken, daha yüksek güvence gerektiren bir ilke içinse, kişinin kendisini uygun bir tanıtma biçimiyle tanımlamasını sağlayacak bir etkinleştirme kodu talep edilebilmektedir. Organizasyonun ihtiyaçlarına ve ilkelerine bağlı olarak, kullanıcının yetki ve erişim kontrol gereksinimleri de göz önüne alınarak, bu iki güvence düzeyinden herhangi birisi kullanılabilir.

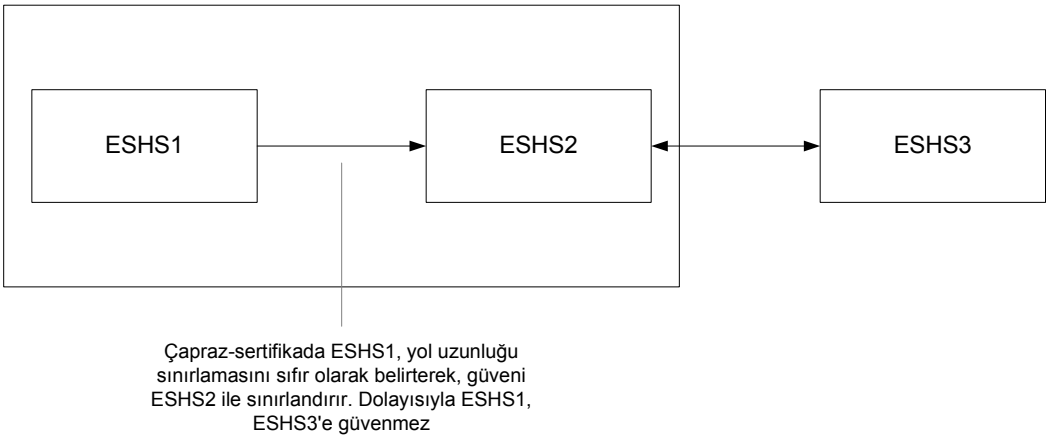
A kuruluşu, B kuruluşundaki sadece yüksek güvence düzeyine sahip kullanıcılar ile güven ilişkisi kurmak üzere çapraz-sertifikasyon sağlamak istiyorsa, ilke sınırlamaları bu amaçla gerçekleştirilebilmektedir (Şekil 17).



Şekil 17 İlke Sınırlaması

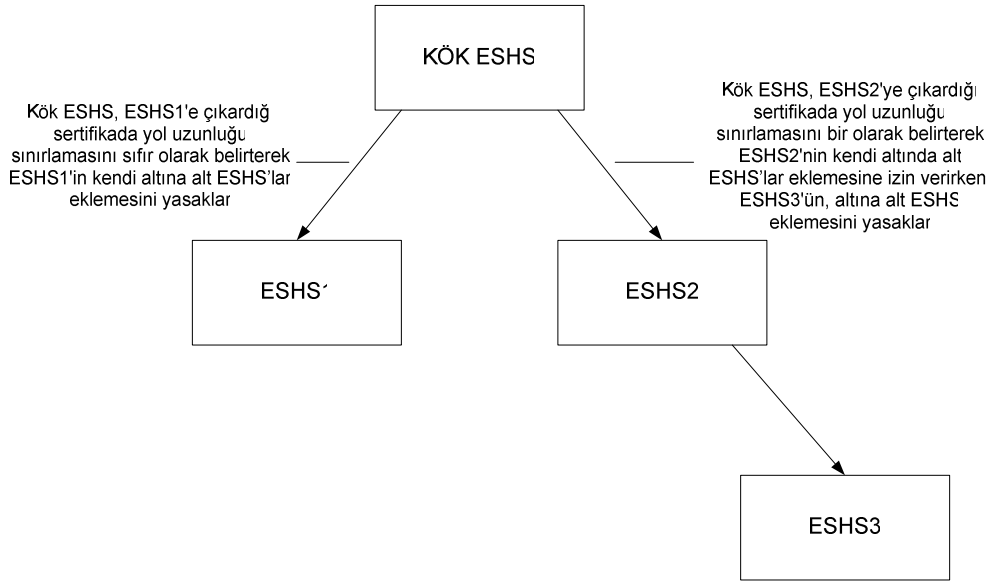
7.1.3.1.3 Yol Uzunluğu Sınırlamaları

Yol uzunluğu sınırlamaları, eş-düzeyli çapraz-sertifikasyonda, geçişli güveni kontrol altında tutmak üzere kullanılabilir (Turnbull, 2000). Çapraz-Sertifikasyon ilişkisine sahip olduğunuz bir ESHS ile kurulmuş bulunan diğer Çapraz-Sertifikasyon ilişkilerine güven duyup duymayacağınız kontrol altına alınır. Şekil 18'de verilen örnekte; ESHS1, ESHS2 ile tek yönlü Çapraz-Sertifikaya sahip, ESHS2 ile ESHS3 ise birbirine çift yanlı Çapraz-Sertifikaya sahiptir.



Şekil 18 Yol Uzunluğu Sınırlaması

Hiyerarşik Çapraz-Sertifikasyonda yol uzunluğu sınırlamaları, alt ESHS'lerin eklenmesi durumunu kontrol altına almak üzere kullanılır. Hiyerarşinin tüm üyeleri birbirlerine güvendiği için bu kontrol, Hiyerarşik Çapraz-Sertifikasyonda oldukça önemlidir. Şekil 19'da örnek bir Hiyerarşik Çapraz-Sertifikasyon yapısında yol uzunluğu sınırlamaları gösterilmiştir**.**



Şekil 19 Hiyerarşik Çapraz Sertifikasyon Yapısı

7.1.3.2 Köprü ESHS

Köprü ESHS, "merkez-ve-konuşma" diye de adlandırılan özel bir güven modeline dayanır. Ve kendisine üye olan ESHS'ler arasında "güven aracısı" olarak işlev görerek bu ESHS'lerin birbirini tanımasını kolaylaştırır (Şekil 20). Köprü ESHS'ler, etki alanları arasındaki karşılıklı çalışabilirlik için geçerli eğilim olarak Çapraz-Sertifikasyon kullanırlar (Lloyd, 2001).

Çapraz-Sertifikasyonun ESHS'lerin birbirleri arasında iki yönlü uygulanmasının ortaya çıkardığı en önemli sorunlardan birisi ölçeklenebilme problemidir. Az sayıda ESHS arasında iki yanlı Çapraz-Sertifikasyon kurulsa bile, bu durum oldukça önemsenecek bir yük getirebilmektedir. Köprü ESHS uygulanarak, bu yük ciddi anlamda azaltılabilir. ESHS'ler birbirleri ile iki yanlı Çapraz-Sertifikasyon kurmak yerine, Köprü ESHS ile bir veya birden fazla sertifika ilkesi kullanarak Çapraz-Sertifikasyon sağlarlar. Sertifika ilkelerinin eşleşmesi durumunda, Köprü ESHS üzerinden ESHS'ler arasında bir güvenilen yol ortaya çıkar.

Şekil 20 Köprü ESHS

- Gerçekleştirilmiş bazı Köprü ESHS'ler aşağıda verilmiştir:
- Federal Bridge CA (ABD)
- DoD Bridge CA (ABD Savunma Birimi)
- EuroPKI (İtalya)
- European Bridge CA (Almanya)

7.1.3.3 Çapraz Tanıma

Çapraz-Tanıma, tanımlı bir kullanıcı topluluğunun, başka bir ESHS tarafından çıkarılan sertifikalara, belirli uygulamalarda kullanmak üzere güven duyabilmesi durumudur (Wilson, 2001). Çapraz-Tanıma, Çapraz-Sertifikasyon ile birkaç bakımdan farklılığa sahiptir. Örneğin, ESHS'ler arasında iki yanlı tanınma söz konusu değildir. Diğer farklılıklardan bir diğeri ise, güven kararlarını ESHS'lerin değil, güvenen kısmın kendisinin yapmasının beklenmesidir (Lloyd, 2001). Çapraz-Tanıma, yüksek düzeyde güvencenin gerekli olduğu durumlarda pek kabul edilebilir çözüm olarak görünmemektedir.

7.1.3.4 Sertifika Güven Listeleri

Sertifika Güven Listesi (SGL), güvenilen ESHS'leri içeren listedir. Güvenilen bir ESHS'nin genel anahtar sertifikasının bir özeti, Sertifika Güven Listesi içerisinde tanıtılır. SGL'ler, ilke tanımlayıcılarını ve eklentilerin kullanım desteğini de içerir. SGL'lerin güvenen tarafa taşınması için tanımlanmış bazı yöntemlerin dışında bant-dışı dağıtım mekanizması da kullanılabilmektedir (Lloyd, 2001).

7.1.3.5 Akreditasyon Sertifikası

ESHS'ler arasında karşılıklı çalışabilirlik için çapraz-sertifikasyon ve çapraz-tanıma ile karşılaşılan bazı sorunların yaşanmaması için Geçiş Denetimi Akreditasyon Sertifikası uygulanabilir. Bu Akreditasyon Sertifikası, ulusal bazda kamu kurumları arasında merkezi ESHS tarafından akredite edilen ESHS'ler için verilebileceği gibi, uluslararası boyutta da verilebilmektedir. Temel olarak, akredite edilmiş ESHS, akredite eden ESHS tarafından imzalanan kendi genel anahtarına sahip olmaktadır (Lloyd, 2001).

Görünüşte, bir sonraki maddede bahsedilecek olan kök hiyerarşi kavramına çok benzese de, kök hiyerarşiden iki önemli farkı vardır. Birincisi, akredite edilmiş her ESHS'nin her biri kendisine has Sertifika İlkeleri ve Sertifika Uygulama Esaslarına sahip olabilmektedir. Diğeri de, ESHS'lerin, mutlak hiyerarşide genellikle izin verilmeyen kendi-imzalı genel anahtar sertifikasına sahip olabilmesine engel durumun olmamasıdır. Dolayısı ile, akredite edilmiş ESHS'ler özerk yapılardır.

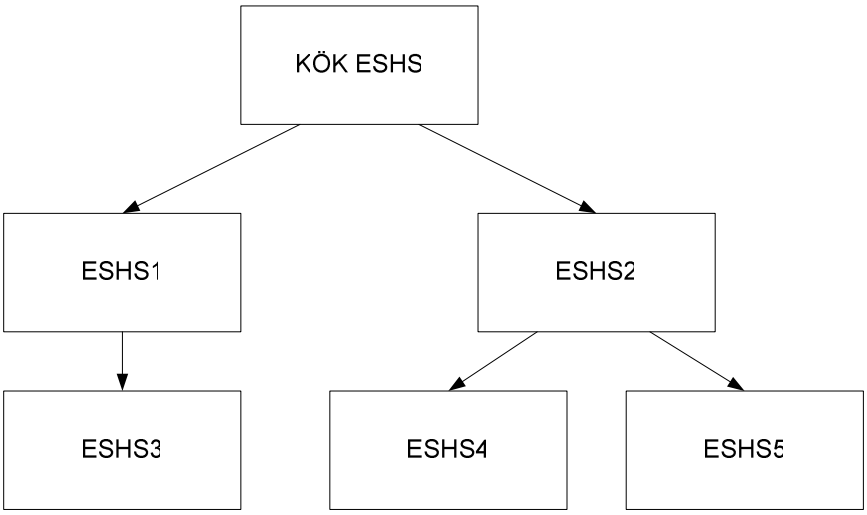
Akreditasyon Sertifikası, Çapraz-Tanımada olduğu gibi, Çapraz-Sertifika yayınlanmasını gerektirmez. Akreditasyon işlemi, akredite edecek ESHS'nin tanımladığı kriterlere göre gerçekleştirilir.

7.1.3.6 Mutlak Hiyerarşi

Mutlak Hiyerarşide, tüm "güven" ortak bir kök ESHS'den çıkar. Dolayısı ile, etki alanındaki tüm güvenen taraflar için kök ESHS, güven noktasıdır. Alt ESHS'ler gerçekleştirilebiliyor olsa da, kök ESHS'ya dayandırılmış olmadığı takdirde alt ESHS'den yayınlanan herhangi bir sertifikaya güven duyulmayacaktır. Alt ESHS'lerin kendi-imzalı sertifikasına sahip olmasına izin verilmez, sadece kök ESHS kendi-imzalı sertifikasına sahip olabilir (Lloyd,2001).

Mutlak Hiyerarşideki yapılar bir kök ESHS ve sıfır veya daha fazla alt ESHS'den oluşur. Şekil 21'de örnek bir Mutlak Hiyerarşi yapısı gösterilmiştir. Bu

örnekte, kök ESHS sertifikaları iki alt ESHS'ye (ESHS1 Ve ESHS2) yayınlar ve daha sonra bu ESHS'ler de kendi alt ESHS'lerine sertifika yayınlarlar. En üstteki ESHS'nin yayınladığı sertifika, aslında iki-yanlı Çapraz-Sertifikadır.



Şekil 21 Mutlak Hiyerarşi

7.1.3.7 Vekillendirilmiş Yol Onaylama ve Bulma

Vekillendirilmiş yol onaylama, güven kararlarını güvenilen taraftan kısmen veya tamamen kaldırmaya izin verir. Bu da, istemci tarafında, güvenilen taraf gibi davranan ve gerektiğinde güvenilen bir üçüncü-parti sunucuya sorgu gerçekleştiren bir yazılım gerektirir. Güvenilen uzak sunucuya "bu sertifikaya güvenmeli miyim?" gibi basit bir istek sorgusu gönderilebildiği gibi, daha karmaşık sorgular da gerçekleştirilebilmektedir. Bu fonksiyonu desteklemek üzere tanımlanan herhangi bir protokol, istek içerisinde farklı düzeylere izin vermelidir (Lloyd, 2001).

Bu konuyu şekillendirmek üzere İnternet Görev Gücü (IETF) tarafından çalışmalar yapılmaktadır. Çevrimiçi Sertifika Durum Protokolü'nün ikinci versiyonu (On-Line Certificate Status Protocol – OCSP) ve ilişkili yol vekillendirme ve onaylama İnternet Taslaklarında belirtilen metodlar ile bu durum başarılabilir. Diğer bir alternatif de, Basit Sertifika Onaylama Protokolü'dür (Simple Certificate Validation Protocol – SCVP). IETF'nin bu alternatiflerden birisini benimseyeceği beklenmektedir.

Bu seçenek her ne kadar, güvenen taraf ile güvenilen taraf arasında bilginin taşınması ve işlenmesi ile ilgili karmaşıklığı azaltması açısından cazip görünse de, bu uyumu sağlamak üzere gerçekleştirilecek arka-uç altyapısı oldukça karmaşıktır.

7.1.4 Uluslararası Durum

Çeşitli ülkeler kendi içlerinde e-imza kullanımının yaygınlaşması ve sorunsuz işlemesi için gerekli hukuksal düzenlemeleri yeni tamamlamış durumdalar, ya da henüz üzerinde çalışıyorlar. Bu nedenle genel kabul görmüş bir uluslararası e-imza standardından söz etmek olası değil. Avrupa Birliği bünyesinde 1999 yılında Avrupa Parlamentosu tarafından yayınlanan AB Elektronik İmza Yönergesi e-imzanın uluslararası geçerliliğinin teşvik edilmesini desteklemektedir. Yönerge, bununla

birlikte, özellikle e-devlet uygulamalarında ülkelerin e-imza sertifikaları için kendilerine özgü ek koşullar tanımlayabileceklerini de belirtmektedir.

8 Güvenlik Elektronik İmzalama Araçları

Bir elektronik imza uygulamasında, elektronik imzanın oluşturulması ve bu imzanın doğrulanmasından bahsedilebilir. Yasada Madde 6'da belirtilen elektronik imza oluşturma verisi, elektronik imzalama amacıyla kullanılan kriptografik özel anahtardır. Aynı şekilde Madde 7'de bahsedilen elektronik imza doğrulama verisi ise elektronik imzayı doğrulama amacıyla kullanılan kriptografik açık anahtardır.

5070 nolu Elektronik İmza yasasına göre, elektronik imza uygulamalarında elektronik imza üretmek için *Güvenli Elektronik İmza Oluşturma Aracı*, varolan bir elektronik imzayı doğrulamak için Güvenli *Elektronik İmza Doğrulama Aracı* kullanılır. Bu iki amaç için kullanılan cihazlara metin boyunca genel olarak "Güvenli Elektronik İmza Aracı" (GEİA) denecektir.

Yasada ve tebliğde tarif edilen şartlara uyan güvenli elektronik imza aracı olarak bugün en yaygın olarak akıllı kartlar (ing. Smartcard) ve akıllı çubuk (ing. Token) kullanılmaktadır.

8.1 GEİA'nın Özellikleri

Akıllı kartlar günümüzde birçok uygulama alanında karşımıza çıkmaktadır. Bir üniversitedeki tüm otomasyonu sağlamak amacıyla kullanılabileceği gibi, yemek çekleri ya da manyetik telefon kartları yerine de kullanılabilmektedir (Şekil 22). Kullandığımız cep telefonları içindeki SIM kart da bir akıllı karttır. Dünyanın en büyük üç kredi kartı üreticisi olan Europay, Mastercard ve Visa'nın ortak kararı ile dünya üzerindeki bu markaların tüm kredi kartlarının 2006 yılından itibaren birer akıllı karta dönüştürülmesi projesi de yakın zamanda gerçekleşecek en büyük akıllı kart dağıtımlarından biri olacaktır. Çubuklar da giderek yaygınlaşan ve kapasiteleri artan taşınabilir birer disk olarak günlük hayatımıza girmeye başlamıştır[1] (Şekil 23).

Şekil 22 Akıllı Kart

Şekil 23 Akıllı Çubuk

[1] 1 GB'a kadar taşınabilir çubuk bellekler mevcuttur.

Tarihsel olarak akıllı kart teknolojisinin gelişimi akıllı çubuğa göre daha eskilere dayanır. Elektronik imza amacıyla kullanılmaya başlanmadan önce, akıllı kartlar, yukarıda sayılanlara benzer birçok uygulama alanını kendilerine bulmuşlardır. Görüntü olarak aynı gibi görünse de kullanılacağı uygulamaya göre bir akıllı kartın ya da çubuğun işlevleri farklılık gösterir. Kontörlü telefon kartı olarak, elektronik imzalama aracı olarak, elektronik ödeme amaçlı olarak, kapı giriş kartı olarak veya bilgisayara kullanıcı girişi sırasında kullanılan akıllı kartlar hem fiyat olarak hem de içerdikleri fonksiyonlar açısından birbirinden farklıdır.

Aynı şekilde taşınabilir disk olarak kullanılan bir çubuk ile elektronik imza aracı olarak kullanılan çubuğun kullandığı teknolojiler birbirinden farklıdır.

8.2 Akıllı Kart ve Akıllı Çubuğun Birbirinden Farkı

Akıllı kartların kullanımı için bir akıllı kart okuyucuya ihtiyaç vardır. Çubuk ise artık birçok bilgisayarda bulunan USB arabirimi üzerinden bilgisayara bağlanabilir. Bunun yanında akıllı kartlar, üzerlerinden farklı uygulamalarda kullanılmak üzere birden çok elektronik devre barındırabilirler. Örneğin bilgisayara giriş için kullanılan bir akıllı kart, elektronik kapı kilitlerini açmakta da kullanılabilir (Bkz. Şekil 24).

Şekil 24 Akıllı Kartların Kullanımı

8.3 GEİA'nın Uyması Gereken Özellikleri

Elektronik imzalama amacıyla kullanılacak akıllı kart/çubuk Güvenli Elektronik GEİA şu standartlara uygun olmalıdırlar (Tebliğ Madde 8, 11b)

- CWA 14169
- TS ISO/IEC 15408 veya ISO/IEC 15408'e göre en az EAL4+

Yasaya göre "Güvenli Elektronik İmza Doğrulama Araçları" ise şu standarda uygun olmalıdırlar:

- CWA 14171

8.4 GEİA nasıl kullanılır?

Bu bölümde herhangi bir elektronik imza uygulamasının GEİA ile ilgili kısımları kabaca tarif edilmiştir.

GEİA'nın bir elektronik imza uygulamasında kullanımında genel olarak iki aşamadan söz edilebilir:

- Kullanıcının uygulamayı kullanmak üzere kaydedilmesi
- Akıllı kartın kişiselleştirilmesi
- Akıllı kartın kullanımı
- Beklenmeyen durumların kotarılması

8.5 Kullanıcının Uygulamayı Kullanmak Üzere Kaydedilmesi

Elektronik imza uygulamasını kullanacak belli bir kullanıcı grubu vardır. Bu kullanıcı grubu örneğin, bir kamu kurumuna ait bir iç uygulamada kurumun personeli, bir kamu kurumunun vatandaşın kullanımına yönelik olarak hazırladığı bir uygulamada ise vatandaşlar olacaktır. Uygulmayı kullanacak olanlar için mutlaka bir kullanıcı kaydı oluşturularak bu kullanıcılar için en az bir elektronik imza oluşturma ve doğrulama verisi çifti (yani kullanıcının açık ve özel anahtar çifti) oluşturulmalıdır.

8.6 Akıllı Kart/USB Çubuk'un Kullanıcılar İçin Kişiselleştirilmesi

Kullanıcının sahip olduğu elektronik imza üretme verisi (yani kullanıcının özel anahtarı), akıllı kartının içerisinde üretilecektir. Yasaya göre bu imza üretme verisi hiçbir şekilde kopyalanamamalı, erişilememeli ve akıllı kart/usb çubuk dışına çıkmamalıdır. Akıllı karta verilen bir komutla anahtar çifti, birkaç saniye süren bir işlem ile karmaşık matematiksel fonksiyonlar sonucunda üretilir. Bu çiftin sadece açık anahtar olacak olan üyesi, akıllı kart dışına çıkarılarak, bir elektronik sertifika oluşturmakta kullanılır. Bu işlem sonucunda akıllı kartın kullanıcı için "*kriptografik olarak kişiselleştirilmesi*" sağlanmış olur.

Kullanıcıya verilecek olan kartın üzerine kullanıcıya özel bilgiler de yazılabilir. Bu işlem için kart üzerine yazma yeteneğine sahip özel yazıcılar kullanılır. İstenilen her türlü bilgi kartın her iki yüzüne de basılabilir. USB çubuklar için böyle bir kişiselleştirme yapma şansı yoktur. Bu işleme de "*Görsel Kişiselleştirme*" denir. Bu işlemlerden sonra kart, kullanıcıya güvenli bir yolla iletilmelidir.

8.7 Akıllı Kartın/Çubuğun Kullanımı

Kullanıcı elektronik imzasını atmak istediği zaman akıllı kartını kullanacaktır. Elektronik imzanın atılması demek, aslında akıllı kart üzerinde bulunan bir elektronik imza fonksiyonuna, yine akıllı kartta bulunan özel anahtar ile imzanacak dökümanın kriptografik olarak özetlenmiş halinin verilmesi ve bu fonksiyondan sonuç olarak imza bilgisinin oluşturulmasıdır. Burada en önemli nokta, imzalama işlemi kart üzerinde yapılabildiğinden, özel anahtarın kart dışına çıkması gerekmemektedir.

8.8 Ayrıcalıklı Durumların Kotarılması

ESHS tarafından, kullanıcının kartını kaybetmesi, kartı kullanırken ihtiyacı olan parola bilgisini unutması, çaldırması, kartın istenmeden zarar görmesi gibi durumlar için yeteri kadar ayrıntılandırılmış prosedürler oluşturulmalı ve uygulanmalıdır. Bu konuda ayrıntılı bilgiler, her ESHS'nin yayınlamakla yükümlü olduğu Sertifikasyon İlkeleri ve Sertifika Uygulama Esasları belgelerinde bulunabilir. Bu konularda ESHS tarafından açık bir nokta ve tanımlanmamış bir durum bırakılmamalıdır. Çünkü bir GEİA'nın kaybolması durumunda, bir kredi kartının kaybolmasından daha vahim sonuçlar oluşabilir

8.9 Elektronik İmza Destekli Kamu Uygulamalarındaki Artışın GEİA Kullanımı Üzerinde Yaratacağı Etki

Yasaya göre, elektronik sertifikalar şahıslar için üretilebilir. Elektronik imza uygulamaları yaygınlaşmaya başladıkça, bir kişinin kullanabildiği uygulamaların sayısı zaman içinde artacaktır. Bu durumda tek bir elektronik sertifika ile birden çok uygulamaya bağlanma gerekliliği ortaya çıkacaktır. Her uygulama geliştiren kurum, kendi uygulamasını kullanacak kullanıcılar için yeni baştan elektronik sertifika üretme sürecini başlatmayacak ve kullanıcının halihazırda sahip olduğu bir elektronik sertifika varsa, bunu kullanılması sağlanacaktır. Elektronik sertifikalar, Yönetmelik'in 11. maddesinde belirtildiği gibi, kurum içi uygulamalar dışında, açık ağlar üzerinden herkes tarafından erişebilecek şekilde konumlandırılacaktır. Böylece elektronik imza doğrulama işlemi için belli bir kişinin elektronik sertifikasına her kurum ve her kişi erişebilecektir. Böylece elektronik imza, uygulamadan bağımsız olarak ancak kişiye bağımlı halde kullanılmış olacaktır.

EK-A

ELEKTRONİK İMZA KANUNU

23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete

Kanun No. 5070 Kabul Tarihi : 15.1.2004

BİRİNCİ KISIM

Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1.- Bu Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.

Kapsam

MADDE 2.- Bu Kanun, elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

Tanımlar

MADDE 3.- Bu Kanunda geçen;

a) Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,

b) Elektronik imza: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi,

c) İmza sahibi: Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi,

d) İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri,

e) İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,

f) İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri,

g) İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını,

h) Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı,

ı) Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,

j) Kurum: Telekomünikasyon Kurumunu, ifade eder.

İKİNCİ KISIM

Güvenli Elektronik İmza ve

Sertifika Hizmetleri

BİRİNCİ BÖLÜM

Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Güvenli elektronik imza

MADDE 4.- Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı

MADDE 5.- Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur.

Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

Güvenli elektronik imza oluşturma araçları

MADDE 6.- Güvenli elektronik imza oluşturma araçları;

a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

Sağlayan imza oluşturma araçlarıdır.

Güvenli elektronik imza doğrulama araçları

MADDE 7.- 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.

İKİNCİ BÖLÜM

Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar

Elektronik sertifika hizmet sağlayıcısı

MADDE 8.- Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak,

İle ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

Kurum, yukarıdaki şartlardan birinin eksikliğini veya yerine getirilmediğini tespit ederse, bu eksikliklerin giderilmesi için, elektronik sertifika hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verir, bu süre içinde elektronik sertifika hizmet sağlayıcısının faaliyetlerini durdurur. Sürenin sonunda eksikliklerin giderilmemesi halinde elektronik sertifika hizmet sağlayıcısının faaliyetine son verir. Kurumun bu kararlarına karşı 19 uncu maddenin ikinci fıkrası hükümleri gereğince itiraz edilebilir.

Elektronik sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında bu maddede gösterilen şartları kaybetmeleri hâlinde de yukarıdaki fıkra hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcıları, Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır.

Nitelikli elektronik sertifika

MADDE 9.- Nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

Bulunması zorunludur.

Elektronik sertifika hizmet sağlayıcısının yükümlülükleri

MADDE 10.- Elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle,

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle,

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla,

e) 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,

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

g) Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmekle,

Yükümlüdür.

Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

Nitelikli elektronik sertifikaların iptal edilmesi

MADDE 11.- Elektronik sertifika hizmet sağlayıcısı;

a) Nitelikli elektronik sertifika sahibinin talebi,

b) Sağladığı nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,

c) Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,

Durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur.

Elektronik sertifika hizmet sağlayıcısı, faaliyetine son vermesi ve vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısı tarafından kullanımının sağlanamaması durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Elektronik sertifika hizmet sağlayıcısının faaliyetine Kurum tarafından son verilmesi halinde Kurum, faaliyetine son verilen elektronik sertifika hizmet sağlayıcısının vermiş olduğu nitelikli elektronik sertifikaların başka bir elektronik sertifika hizmet sağlayıcısına devredilmesine karar verir ve durumu ilgililere duyurur.

Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez.

Bilgilerin korunması

MADDE 12.- Elektronik sertifika hizmet sağlayıcısı;

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

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

Hukukî sorumluluk

MADDE 13.- Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir.

Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.

Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz.

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.

Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenir.

Bu maddede öngörülen sertifika malî sorumluluk sigortası Türkiye'de ilgili branşta çalışmaya yetkili olan sigorta şirketleri tarafından yapılır. Bu sigorta şirketleri sertifika malî sorumluluk sigortasını yapmakla yükümlüdürler. Bu yükümlülüğe uymayan sigorta şirketlerine Hazine Müsteşarlığınca sekizmilyar lira idarî para cezası verilir. Bu para cezasının tahsilinde ve cezaya itiraz usulünde 18 inci madde hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür.

Yabancı elektronik sertifikalar

MADDE 14.- Yabancı bir ülkede kurulu bir elektronik sertifika hizmet sağlayıcısı tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir.

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.

ÜÇÜNCÜ KISIM

Denetim ve Ceza Hükümleri

Denetim

MADDE 15.- Elektronik sertifika hizmet sağlayıcılarının bu Kanunun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Kurumca yerine getirilir.

Kurum, gerekli gördüğü zamanlarda elektronik sertifika hizmet sağlayıcılarını denetleyebilir. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.

İmza oluşturma verilerinin izinsiz kullanımı

MADDE 16.- Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve beşyüz milyon liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

Elektronik sertifikalarda sahtekârlık

MADDE 17.- Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullananlar, fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve birmilyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.

Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

İdarî para cezaları

MADDE 18.- Bu Kanunun;

a) 10 uncu maddesindeki yükümlülüklerinden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına onmilyar lira,

b) 11 inci maddesindeki yükümlülüklerden herhangi birini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

c) 12 nci maddesi hükümlerine aykırı hareket edenler hakkında onmilyar lira,

d) 13 üncü maddesinin beş ve yedinci fıkralarındaki yükümlülükleri yerine getirmeyen elektronik sertifika hizmet sağlayıcısına sekizmilyar lira,

e) 15 inci maddesi hükmüne aykırı hareket eden elektronik sertifika hizmet sağlayıcısına yirmimilyar lira,

İdarî para cezası Telekomünikasyon Kurulu tarafından verilir. Verilen para cezalarına dair kararlar ilgililere 7201 sayılı Tebligat Kanunu hükümlerine göre tebliğ edilir. Bu cezalara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, verilen cezanın yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir. Bu Kanuna göre verilen idarî para cezaları, Kurumun bildirimi üzerine 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümlerine göre Maliye Bakanlığınca tahsil olunur.

İdarî nitelikteki suçların tekrarı ve kapatma

MADDE 19.- 18 inci maddedeki suçları işleyenlerin bu suçları işledikleri tarihten itibaren geriye doğru üç yıl içinde ikinci kez işlemeleri hâlinde para cezaları iki kat olarak uygulanır, üçüncü kez işlemeleri hâlinde ise Kurum tarafından elektronik sertifika hizmet sağlayıcıları hakkında kapatma cezası verilir.

Kapatma cezası verilmesine ilişkin karar 7201 sayılı Tebligat Kanununa göre ilgililere tebliğ edilir. Bu karara karşı tebliğ tarihinden itibaren en geç yedi gün içinde yetkili idare mahkemesine itiraz edilebilir. İtiraz, yetkili makam tarafından verilen kapatma kararının yerine getirilmesini durdurmaz. İtiraz, zaruret görülmeyen hâllerde, evrak üzerinden inceleme yapılarak en kısa sürede sonuçlandırılır. İtiraz üzerine verilen kararlara karşı Bölge İdare Mahkemesine başvurulabilir. Bölge İdare Mahkemesinin verdiği kararlar kesindir.

DÖRDÜNCÜ KISIM

Çeşitli Hükümler

Yönetmelik

MADDE 20.- Bu Kanunun 6, 7, 8, 10, 11 ve 14 üncü maddelerinin uygulanmasına ilişkin usul ve esaslar, Kanunun yürürlük tarihinden itibaren altı ay içinde ilgili kurum ve kuruluşların görüşleri alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir.

Kamu kurum ve kuruluşları hakkında uygulanmayacak hükümler

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

MADDE 22.- 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir.

Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir.

MADDE 23.- 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmiştir.

MADDE 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır.

MADDE 24.- 5.4.1983 tarihli ve 2813 sayılı Telsiz Kanununun 7 nci maddesinin birinci fıkrasına aşağıdaki (m) bendi eklenmiş ve mevcut (m) bendi (n) bendi olarak teselsül ettirilmiştir.

m) Elektronik İmza Kanunu ile verilen görevleri yerine getirmek,

Yürürlük

MADDE 25.- Bu Kanun yayımı tarihinden altı ay sonra yürürlüğe girer.

Yürütme

MADDE 26.- Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

Telekomünikasyon Kurumundan: **EK-B**

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

Madde 1 — Bu Tebliğin amacı, elektronik imzaya ilişkin süreçleri ve teknik kriterleri detaylı olarak belirlemektir.

Kapsam

Madde 2 — Bu Tebliğ; nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve hizmetlerine ilişkin teknik hususları kapsar.

Dayanak

Madde 3 — Bu Tebliğ, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 34 üncü maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4 — Bu Tebliğde geçen;

Yönetmelik: Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliği,

BS (British Standards): İngiliz Standartlarını,

CEN (Comité Européen de Normalisation): Avrupa Standardizasyon Komitesini,

CWA (CEN Workshop Agreement): CEN Çalıştay Kararını,

DSA (Digital Signature Algorithm): Sayısal İmza Algoritmasını,

DSA Eliptik Eğrisi (DSA Elliptical Curve): Sayısal İmza Algoritması Eliptik Eğrisini,

EAL (Evaluation Assurance Level): Değerlendirme Garanti Düzeyini,

ETSI (European Telecommunications Standards Institute): Avrupa Telekomünikasyon Standartları Enstitüsünü,

ETSI SR (ETSI Special Report): ETSI Özel Raporunu,

ETSI TS (ETSI Technical Specification): ETSI Teknik Özelliklerini,

FIPS PUB (Federal Information Processing Standards Publications): Federal Bilgi İşleme Standartları Yayınlarını,

IETF RFC (Internet Engineering Task Force Request for Comments): İnternet Mühendisliği Görev Grubu Yorum Talebini,

ISO/IEC (International Organisation for Standardisation / International Electrotechnical Commitee): Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesini,

ITU (International Telecommunication Union): Uluslararası Telekomünikasyon Birliğini,

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): RACE Bütünlük Asli Mesaj Değerlendirme Özetini,

RSA: Rivest-Shamir-Adleman'ı,

SHA (Secure Hash Algorithm): Güvenli Özet Algoritmasını ifade eder.

Bu Tebliğde yer almayan tanımlar için Kanun ve Yönetmelikte yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM

Teknik Hususlar

ESHS'nin İşleyişi

Madde 5 — ESHS işleyişinin bütün aşamalarında;

a) ETSITS 101 456 ve

b) CWA 14167-1

standartlarına uyar.

Nitelikli elektronik sertifikalar;

a) ETSITS 101 862 ve

b) ITU-TRec. X.509V.3'e

uygun olarak oluşturulur.

Algoritmalar ve Parametreler

Madde 6 — İmza oluşturma ve doğrulama verileri, aşağıda belirtilen algoritma ve parametrelere uygun olarak oluşturulur;

a) İmza sahibinin imza oluşturma ve doğrulama verileri

i. RSA için en az 1024 bit veya

ii. DSA için en az 1024 bit veya

iii. DSA Eliptik Eğrisi için en az 160 bit

b) ESHS'nin imza oluşturma ve doğrulama verileri

i. RSA için en az 2048 bit veya

ii. DSA için en az 2048 bit veya

iii. DSA Eliptik Eğrisi için en az 256 bit Özetleme algoritması olarak;

a) RIPEMD-160 veya

b) SHA-1

kullanılır.

Yukarıda belirtilen algoritmalar ve parametreler 31/12/2005 tarihine kadar geçerlidir.

Yukarıda belirtilen algoritmalara ve parametrelere bağlı kalmak şartı ile ETSI SR 002 176 raporunda belirtilen imza oluşturma ve doğrulama verilerinin oluşturulmasında kullanılan algoritma ve parametreler de geçerlidir.

Sertifika İlkeleri ve Sertifika Uygulama Esasları

Madde 7 — ESHS; sertifika ilkelerini ve sertifika uygulama esaslarını IETF RFC 3647'ye uygun olarak hazırlar.

Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Madde 8 — Güvenli 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 EAL4+ seviyesinde olmalıdır.

ESHS, sağlamış olduğu güvenli elektronik imza doğrulama araçları için CWA 14171 standardına uyar ve bunu yazılı olarak taahhüt eder.

Güvenlik Kriterleri

Madde 9 — ESHS, güvenlik kriterlerine ilişkin olarak;

a) CWA 14167-1,

b) ETSITS 101 456 ve

c) TS ISO/IEC 17799 veya ISO/IEC 17799

standartlarına uyar.

Zaman Damgası ve Hizmetleri

Madde 10 — 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.

Belgeler

Madde 11 — ESHS;

a) BS 7799-2 standardına uygunluğunu,

b) Güvenli elektronik imza oluşturma araçlarının;

i. FIPS PUB 140-1 veya FIPS PUB 140-2'ye göre seviye 3 veya üzerinde olduğunu veya

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

iii. CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olduğunu

yetkili kurum veya kuruluşlardan alman belgelerle belgelendirir.

ÜÇÜNCÜ BÖLÜM

Diğer Hükümler

Yürürlük

Madde 12 — Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 13 — Bu Tebliğ hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.

EK-C

Genelge

Başbakanlıktan:

Konu: Kamu Sertifikasyon Merkezi Oluşturulması.

Genelge

2004/21

23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanarak, 23 Temmuz 2004 tarihinde yürürlüğe girmiş bulunan 5070 sayılı Elektronik İmza Kanunu ile güvenli elektronik imzanın elle atılan imza ile aynı ispat gücüne sahip olduğu ve bu şekilde oluşturulan elektronik verilerin hukuken geçerli olacağı hususları düzenlenmiştir.

Kanun ile yapılan düzenlemeler, kamu kurum ve kuruluşlarının kendi aralarında yapacakları iletişimin yanı sıra, vatandaşlar ve iş alemi ile arasındaki iletişimin niteliğini, güvenilirliğini, etkinliğini ve hızını da büyük oranda ve olumlu yönde etkileyecektir. Elektronik imzanın sağlayacağı imkanlardan yararlanabilmek için, kamu çalışanları da dahil olmak üzere, vatandaşların, Kanun'da belirtilen nitelikleri haiz bir elektronik sertifika hizmet sağlayıcısından elektronik sertifika temin etmeleri yeterli olacaktır.

Diğer taraftan, kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaya çalıştıkları gözlenmektedir. Bu münferit çalışmaların, bir yandan sistemin kendi işleyişi içerisinde karmaşaya yol açması, diğer yandan da mükerrerliklere ve dolayısıyla emek ve kaynak israfına neden olması kaçınılmazdır.

Yasanın yürürlüğe girmesiyle birlikte ülkemizde de giderek yaygınlaşacak olan elektronik imza uygulamaları kapsamında; kamu kurum ve kuruluşlarının elektronik ortamlarda yürütecekleri iş ve işlemlerde uyumlu, birlikte işler ve güvenilir bir yapıda çalışmasını sağlamak maksadıyla, 10 Haziran 2004 tarihinde yapılan e-Dönüşüm Türkiye İcra Kurulu VI. Toplantısı'nda alınan 6 sayılı İcra Kurulu Kararı ile kamu kurum ve kuruluşlarının elektronik sertifika ihtiyaçlarının tek merkezden sağlanması kararlaştırılmıştır.

Bu kapsamda, tüm kamu kurum ve kuruluşlarının, kurumsal sertifika (kamu çalışanlarınca kurum içi ve kurumlar arası işlemlerde kullanılacak sertifika) ihtiyaçlarının karşılanması amacıyla bir Kamu Sertifikasyon Yapısı oluşturulması kararlaştırılmıştır.

Söz konusu yapı içerisinde, en üst seviyede bir Kök Sertifika Hizmet Sağlayıcısı ile buna bağlı olarak Kamu Sertifika Hizmet Sağlayıcısı kurulacaktır. Yürüttükleri görevler açısından özel niteliği haiz Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, Kamu Sertifika Hizmet Sağlayıcısı sistemlerini kendi bünyelerinde oluşturabileceklerdir. Diğer kamu kurum ve kuruluşları kurumsal sertifikalarını, Kamu Sertifika Hizmet Sağlayıcısından temin edeceklerdir.

Kamu çalışanları, kurumsal sertifikalarını kamu dışı bireysel işlemlerinde de kullanabilecektir.

Kurulacak bu Kamu Sertifikasyon Yapısı içinde yer alan Kök Sertifika Hizmet Sağlayıcısı, dileyen gerçek ve tüzel kişilerin kuracakları Sertifika Hizmet Sağlayıcılarına da kök sertifika hizmeti verebilecektir.

Ulusal güvenlik gerekleri göz önünde bulundurularak, kurumsal sertifika ihtiyacının karşılanması amacıyla oluşturulacak Kamu Sertifikasyon Yapısı içinde kurulacak olan Kök Sertifika Hizmet Sağlayıcısı ve Kamu Sertifika Hizmet Sağlayıcısı milli yazılım ürünlerini kullanacaktır.

Bu kapsamda; tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifikasyon yapısı altında toplanmasını hedefleyen, sadece kamu kurum ve kuruluşlarına kurumsal sertifikaların oluşturulması ve sertifika yaşam çevriminin yönetilmesini sağlayacak Kamu Sertifikasyon Yapısının kurulması ve işletilmesi görev ve sorumluluğu Türkiye Bilimsel ve Teknik Araştırma Kurumu'na bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü'ne (UEKAE) verilmiştir. Söz konusu yapının gözden geçirilmesi ve uygunluğunun izlenmesi görev ve sorumluluğu ise Telekomünikasyon Kurumuna verilmiştir.

Bahse konu Kamu Sertifikasyon Yapısının kurulması için TÜBİTAK-UEKAE tarafından gerekli çalışmalar derhal başlatılacaktır. Bu çerçevede; TÜBİTAK-UEKAE tarafından ihtiyaç duyulacak kaynak tahsisi ve düzenlemelere ilişkin çalışmalar ile kurulacak yapıya uyum için kamu kurum ve kuruluşları nezdinde sürdürülecek çalışmalar, DPT Müsteşarlığının koordinasyonunda yürütülecektir.

Yukarıda belirtilen istisnalar dışındaki kamu kurum ve kuruluşları, sertifika ihtiyaçlarını karşılamak amacıyla Sertifika Hizmet Sağlayıcısı olmak üzere kendi bünyelerinde hiçbir surette yeni yatırım yapmayacaklardır. Bu konuda başlatılmış ve sürdürülmekte olan ihale çalışmaları ile henüz sözleşmeye bağlanmamış olan tüm ihaleler derhal iptal edilecektir. Sözleşmeye bağlanmış olanlardan, tek taraflı fesih hakkı bulunan sözleşmeler derhal feshedilecek, halihazırda kullanılmakta olan sistemler ise Telekomünikasyon Kurumu'nun da görüşü alınmak suretiyle en kısa sürede bu yapıya uygun hale getirilecektir.

Ayrıca; henüz kullanıma geçmemiş olmakla birlikte, çalışmaları devam eden ve sözleşmeleri tek taraflı olarak fesih edilemeyen proje ya da proje bileşenlerine ilişkin karar, DPT Müsteşarlığı ve ilgili kuruluşun ortak çalışması ile sonuçlandırılacaktır.

Kamu kurum ve kuruluşları, bu Genelge çerçevesinde tek taraflı olarak feshettikleri veya tek taraflı fesih hakkı olmayan proje ya da proje bileşenleri konusunda detaylı bilgileri içerecek raporları, Genelge'nin yayımı tarihinden itibaren 15 gün içinde Devlet Planlama Teşkilatı Müsteşarlığına ileteceklerdir.

Bilgilerini ve gereğini rica ederim.

Recep Tayyip ERDOĞAN

Başbakan

EK-D

2 Aralık 2004 PERŞEMBE

Sayı : 25658

RESMİ GAZETE

Resmî Yazışmalarda Uygulanacak Esas ve Usuller Hakkında Yönetmelik

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

Madde 1 — Bu Yönetmeliğin amacı; resmî yazışma kurallarını belirlemek, bilgi ve belge alışverişinin sağlıklı, hızlı ve güvenli bir biçimde yürütülmesini sağlamaktır.

Kapsam

Madde 2 — Bu Yönetmelik, bütün kamu kurum ve kuruluşlarını kapsar.

Dayanak

Madde 3 — Bu Yönetmelik, 10/10/1984 tarihli ve 3056 sayılı Başbakanlık Teşkilatı Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanunun 2 nci ve 33 üncü maddelerine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4 — Bu Yönetmelikte geçen;

a) Resmî yazı: Kamu kurum ve kuruluşlarının kendi aralarında veya gerçek ve tüzel kişilerle iletişimlerini sağlamak amacıyla yazılan yazı, resmî belge, resmî bilgi ve elektronik belgeyi,

b) Resmî belge: Kamu kurum ve kuruluşlarının kendi aralarında veya gerçek ve tüzel kişilerle iletişimlerini sağlamak amacıyla oluşturdukları, gönderdikleri veya sakladıkları belirli bir standart ve içeriği olan belgeleri,

c) Resmî bilgi: Kamu kurum ve kuruluşlarının kendi aralarında veya gerçek ve tüzel kişilerle iletişimleri sırasında metin, ses ve görüntü şeklinde oluşturdukları, gönderdikleri veya sakladıkları bilgileri,

d) Elektronik ortam: Belge ve bilgilerin üzerinde bulunduğu her türlü bilgisayarı, gezgin elektronik araçları, bilgi ve iletişim teknolojisi ürünlerini,

e) Elektronik belge: Elektronik ortamda oluşturulan, gönderilen ve saklanan her türlü belgeyi,

f) Dosya planı: Resmî yazıların hangi dosyaya konulacağını gösteren kodlara ait listeyi,

g) Yazı alanı: Yazı kağıdının üst, alt, sol ve sağ kenarından 2,5 cm boşluk bırakılarak düzenlenen alanı,

h) Güvenli elektronik imza: Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzayı,

ifade eder.

İKİNCİ BÖLÜM
Resmî Yazışma Ortamları, Nüsha Sayısı, Belge Boyutu ve Yazı Tipi

Resmî yazışma ortamları ve güvenlik

Madde 5 — Kamu kurum ve kuruluşları arasında yazılı iletişim, kâğıt kullanılarak veya elektronik ortamda yapılır.

Kâğıtla yapılan resmî yazışmalarda daktilo veya bilgisayar kullanılır. Bu tür yazışmalar, yazının içeriğine ve ivedilik durumuna göre faks ile de gönderilebilir. Faksla yapılan yazışmalarda, yazıda belirtilen hususlarda hemen işlem yapılabilir, ancak bunların beş gün içerisinde resmî yazı ile teyidinin yapılması gerekir.

Elektronik ortamdaki yazışmalar ilgili mevzuatta belirtilen güvenlik önlemlerine uyularak yapılır.

Elektronik ortamda yapılan yazışmalar bu ortamın özellikleri dikkate alınarak kaydedilir, dosyalanır ve ilgili yere iletilir. Gerekli durumlarda, gelen yazı kağıda dökülerek de işleme alınır.

Her kurum kendisi ve gerektiğinde kurum içindeki birimler adına resmî elektronik posta (e-posta) adresi belirler. Bu adreslerin belirlenmesinde koordinasyon Başbakanlık tarafından yapılır. Elektronik ortamdaki resmî yazışmalar bu adresler arasında yapılır.

Kamu kurum ve kuruluşları elektronik ortamda yapılacak yazışmalarda, bu Yönetmeliğe aykırı olmamak kaydıyla gerekli düzenlemeleri yapabilir.

Nüsha sayısı

Madde 6 — Kağıt kullanılarak hazırlanan resmî yazılar en az iki nüsha olarak düzenlenir.

Belge boyutu

Madde 7 — Resmî yazışmalarda A4 (210x297 mm) ve A5 (210x148 mm) boyutunda kağıt kullanılır.

Yazı tipi ve karakter boyutu

Madde 8 — Bilgisayarla yazılan yazılarda "Times New Roman" yazı tipi ve 12 karakter boyutunun kullanılması esastır. Rapor, form ve analiz gibi özelliği olan metinlerde farklı yazı tipi ve karakter boyutu kullanılabilir.

ÜÇÜNCÜ BÖLÜM
Resmî Yazıların Bölümleri

Başlık

Madde 9 — Başlık, yazıyı gönderen kurum ve kuruluşun adının belirtildiği bölümdür. Bu bölümde amblem de yer alabilir.

Başlık, kağıdın yazı alanının üst kısmına ortalanarak yazılır.

İlk satıra "T.C." kısaltması, ikinci satıra kurum ve kuruluşun adı büyük harflerle, üçüncü satıra ise ana kuruluşun ve birimin adı küçük harflerle ortalanarak yazılır. Başlıkta yer alan bilgiler üç satırı geçemez.

Bakanlıklar ile bağlı ve ilgili kuruluşların taşra teşkilatlarında kullanılan başlıklar 5442 sayılı İl İdaresi Kanunu hükümlerine uygun olarak düzenlenir.

Bölge müdürlüklerinde ise bakanlığın adının altına hangi bölge teşkilatı olduğu yazılır (Örnek:1).

Sayı ve evrak kayıt numarası

Madde 10 — Sayı ve evrak kayıt numarası, dosya planına göre verilir, başlığın son satırından iki aralık aşağıda ve yazı alanının en solundaki "Sayı:" yan başlığından sonra yazılır.

Bu ifadeden sonra kod numarası verilir. Kod numarasından sonra kısa çizgi (-) işareti konularak dosya numarası, dosya numarasından sonra (-) işareti konularak evrak kayıt numarası yazılır. Genel evrak biriminden sayı verilmesi durumunda araya eğik çizgi (/) işareti konulur.

Evrak kayıt numarası, yazıyı gönderen birimde ve/veya kurumun genel evrak biriminde aldığı numaradır (Örnek: 2).

Resmî yazışmalarda Başbakanlık tarafından belirlenen kodlama sistemine ve dosya planına uyulması zorunludur.

Tarih

Madde 11 — Yazının yetkili amir tarafından imzalanarak ilgili birimden sayı verildiği zamanı belirten tarih bölümü, sayı ile aynı hizada olmak üzere yazı alanının en sağında yer alır.

Tarih; gün, ay ve yıl rakamla, aralarına (/) işareti konularak yazılır.

Konu

Madde 12 — Konu, sayının bir aralık altına "Konu:" yan başlığından sonra, başlık bölümündeki "T.C." kısaltması hizasını geçmeyecek biçimde yazılır. Yazının konusu, anlamlı ve özlü bir şekilde ifade edilir.

Gönderilen makam

Madde 13 — Gönderilen makam; yazının gönderildiği kurum, kuruluş ve kişi ile bunların bulundukları yeri belirtir. Bu bölüm; konunun son satırından sonra, yazının uzunluğuna göre iki-dört aralık aşağıdan ve kağıdı ortalayacak biçimde büyük harflerle yazılır. Yazının gönderildiği yerin belirlenmesine ilişkin diğer hususlar parantez içinde küçük harflerle ikinci satıra yazılır.

Kuruluş dışına gönderilen yazılarda, gerekiyorsa yazının gideceği yerin adresi küçük harflerle ve başlığın ilk satırının hizasında, iki aralık bırakılarak ayrıca belirtilir.

Kişilere yazılan yazılarda; "Sayın" kelimesinden sonra ad küçük, soyadı büyük, unvan ise küçük harflerle yazılır (Örnek: 3).

İlgi

Madde 14 — İlgi, yazılan yazının önceki bir yazıya ek ya da karşılık olduğunu veya bazı belgelere başvurulması gerektiğini belirten bölümdür.

"İlgi:" yan başlığı, gönderilen makam bölümünün iki aralık altına ve yazı alanının soluna küçük harflerle yazılır.

İlgide yer alan bilgiler bir satın geçerse, "İlgi" kelimesinin altı boş bırakılarak ikinci satıra yazılır.

İlginin birden fazla olması durumunda, a, b, c gibi küçük harfler yanlarına ayraç işareti ") " konularak kullanılır.

İlgide, " tarihli ve sayılı" ibaresi kullanılır.

İlgide yazının sayısı, kurum veya birimin dosya kodu tam olarak belirtilir. İlgi, tarih sırasına göre yazılır. Yazı aynı konuda birden fazla makamın yazısına karşılık veya daha önce yazılmış çok sayıda yazıyla ilgili ise bunların hepsi belirtilir (Örnek: 4).

Metin

Madde 15 — Metin, "İlgi"den sonra başlayıp "İmza"ya kadar süren kısımdır.

Metne, "İlgi"nin son satırından itibaren iki aralık, "İlgi" yoksa gönderilen yerden sonra üç aralık bırakılarak başlanır.

Metindeki kelime aralarında ve nokta, virgül, soru işareti gibi yazı unsurlarının arasında bir vuruş boşluk bırakılır.

Paragraf başlarına yazı alanının 1.25 cm içerisinden başlanır. Paragraf başı yapılmadığı durumlarda paragraflar arasında bir satır aralığı boşluk bırakılır (Örnek: 5-A, B).

Metin içinde geçen sayılar rakamla ve/veya yazı ile yazılabilir. Önemli sayılar rakam ile yazıldıktan sonra parantez içerisinde yazı ile de gösterilebilir.

Metin içinde veya çizelgelerde üçlü gruplara ayrılarak yazılan büyük sayılarda gruplar arasına nokta (22.465.660), sayıların yazılışında kesirleri ayırmak için ise virgül (25,33 -yirmi beş tam yüzde otuz üç) kullanılır.

Yazı, Türk Dil Kurumu tarafından hazırlanan İmla Kılavuzu ile Türkçe Sözlük esas alınarak dil bilgisi kurallarına göre yaşayan Türkçe ile yazılır.

Metinde zorunlu olmadıkça yabancı kelimelere yer verilmez ve gereksiz tekrardan kaçınılır. Türk Dil Kurumu tarafından hazırlanan İmla Kılavuzu'nda bulunmayan kısaltmaların kullanılmasının zorunlu olduğu durumlarda, kısaltmanın ilk kullanıldığı yerde parantez içinde kısaltmanın açık biçimi gösterilir.

Alt makama yazılan yazılar "Rica ederim.", üst ve aynı düzey makamlara yazılan yazılar "Arz ederim.", üst ve alt makamlara dağıtımlı olarak yazılan yazılar "Arz ve rica ederim." biçiminde bitirilir.

İmza

Madde 16 — Metnin bitiminden itibaren iki-dört aralık boşluk bırakılarak yazıyı imzalayacak olan makam sahibinin adı, soyadı ve unvanı yazı alanının en sağına yazılır. İmza ad ve soyadın üzerinde bırakılan boşluğa atılır. Elektronik ortamda yapılacak yazışmalarda, imza yetkisine sahip kişi yazıyı, güvenli elektronik imzası ile imzalar.

Yazıyı imzalayanın adı küçük, soyadı büyük harflerle yazılır. Unvanlar ad ve soyadın altına küçük harflerle yazılır. Akademik unvanlar ismin ön tarafına küçük harflerle ve kısaltılarak yazılır.

Yazıyı imzalayacak olan makam, yazının gideceği makama göre kurum/kuruluşun "imza yetkileri yönergesi"ne veya yetkili makamlarca verilen imza-yetkisine uyularak seçilir.

Yazıyı makam sahibi yerine yetki devredilen kişi imzaladığında, imzalayanın ad ve soyadı birinci satıra, yetki devredenin makamı "Başbakan a.", "Vali a." ve "Rektör a.", biçiminde ikinci satıra, imzalayan makamın unvanı ise üçüncü satıra yazılır.

Yazı vekaleten imzalandığında, imzalayanın ad ve soyadı birinci satıra, vekalet bırakanın makamı "Başbakan V.", "Vali V." ve "Rektör V." biçiminde ikinci satıra yazılır (Örnek: 6-A).

Yazının iki yetkili tarafından imzalanması durumunda üst makam sahibinin adı, soyadı, unvanı ve imzası sağda (Örnek: 6-B); ikiden fazla yetkili tarafından imzalanması durumunda üst makam sahibinin adı, soyadı, unvanı ve imzası solda olmak üzere yetkililer makam sırasına göre soldan sağa doğru sıralanır (Örnek: 6-C).

Atama kararnamelerinde imza bölümü, Örnek: 6-D'de olduğu biçimde düzenlenir.

Onay

Madde 17 — Onay gerektiren yazılar ilgili birim tarafından teklif edilir ve yetkili makam tarafından onaylanır.

Yazı onaya sunulurken imza bölümünden sonra uygun satır aralığı bırakılarak yazı alanının ortasına büyük harflerle "OLUR" yazılır. "OLUR"un altında onay tarihi yer alır.

Onay tarihinden sonra imza için uygun boşluk bırakılarak onaylayanın adı, soyadı ve altına unvanı yazılır (Örnek: 7-A).

Yazıyı teklif eden birim ile onay makamı arasında makamlar varsa bunlardan onay makamına en yakın yetkili "Uygun görüşle arz ederim." ifadesiyle onaya katılır. Bu ifade, teklif eden birim ile onay bölümü arasına uygun boşluk bırakılarak yazılır ve yazı alanının solunda yer alır (Örnek: 7-B).

Elektronik ortamda hazırlanan yazıya onay verecek yetkili kişi resmî yazıyı güvenli elektronik imzası ile imzalar.

Ekler

Madde 18 — Yazının ekleri imza bölümünden sonra uygun satır aralığı bırakılarak yazı alanının soluna konulan "EK/EKLER:" ifadesinin altına yazılır.

Ek adedi birden fazla ise numaralandırılır. Ek listesi yazı alanına sığmayacak kadar uzunsa ayrı bir sayfada gösterilir.

Yazı eklerinin dağıtımdaki bazı yerlere gönderilmediği durumlarda, "Ek konulmadı" ya da "Ek-.... konulmadı", bazı eklerin konulması durumunda ise, "Ek-.... Konuldu" ifadesi yazılır (Örnek: 8).

Dağıtım

Madde 19 — Dağıtım, yazıların gereği ve bilgi için gönderildiği yerlerin protokol sırası esas alınarak belirtildiği bölümdür. "EKLER"den sonra uygun satır aralığı bırakılarak yazı alanının soluna "DAĞITIM:" yazılır. Ek yoksa dağıtım EKLER'in yerine yazılır.

Yazının gereğini yerine getirme durumunda olanlar, "Gereği" kısmına, yazının içeriğinden bilgilendirilmesi istenenler ise "Bilgi" kısmına protokol sırasıyla yazılır. "Gereği" kısmı dağıtım başlığının altına, "Bilgi" kısmı ise "Gereği" kısmı ile aynı satıra yazılır.

"Bilgi" kısmı yoksa, kurum ve kuruluş adları doğrudan "DAĞITIM" başlığının altına yazılır (Örnek: 9-A, B).

Paraf

Madde 20 — Yazının kurum içinde kalan nüshası, yazıyı hazırlayan ve kurum tarafından belirlenen en fazla 5 görevli tarafından paraf edilir. Paraflar, adres bölümünün hemen üstünde ve yazı alanının solunda yer alır.

Elektronik ortamda yapılan yazışmalarda paraflar elektronik onay yoluyla alınır.

Yazıyı paraflayan kişilerin unvanları gerektiğinde kısaltılarak yazılır, (:) işareti konulduktan sonra büyük harfle adının baş harfi ve soyadı yazılır. El yazısı ile tarih belirtilerek paraflanır (Örnek: 10).

Koordinasyon

Madde 21 — Başka birimlerle işbirliği yapılarak hazırlanan yazılarda, paraf bölümünden sonra bir satır aralığı bırakılarak "Koordinasyon:" yazılır ve işbirliğine dahil olan personelin unvan, ad ve soyadları paraf bölümündeki biçime uygun olarak düzenlenir (Örnek: 11).

Adres

Madde 22 — Yazı alanının sınırları içinde kalacak şekilde sayfa sonuna soldan başlayarak yazıyı gönderen kurum ve kuruluşun adresi, telefon ve faks numarası, e-posta adresi ve elektronik ağ sayfasını içeren iletişim bilgileri yazılır. İletişim bilgileri yazıdan bir çizgi ile ayrılır.

Yazının gönderildiği kurum ve kişilerin, gerektiğinde daha ayrıntılı bilgi alabilmeleri için başvuracakları görevlinin adı, soyadı ve unvanı adres bölümünün sağında yer alır (Örnek: 12).

Gizli yazılar

Madde 23 — Yazı gizlilik derecesi taşıyorsa, gizlilik derecesi belgenin üst ve alt ortasına büyük harflerle kırmızı renkli olarak belirtilir. Gizlilik dereceleri; çok gizli, gizli, özel, hizmete özel şeklinde görev alanı ve hizmet özelliğine göre kurum veya kuruluşça belirlenir (Örnek: 5-A, B).

İvedi ve günlü yazılar, tekit yazısı

Madde 24 — Öncelik verilmesi gereken durumlarda yazıya cevap verilmesi gereken tarih metin içinde, yazının ivedi ve günlü olduğu ise sayfanın sağ üst kısmında büyük harflerle kırmızı renkli olarak belirtilir. Yazıyı alan bu ivediliğin gereğini yapmakla yükümlüdür (Örnek: 5-A, B).

Resmî yazılara uygun sürede cevap verilmemesi durumunda ilgili kurum ve kuruluşlara tekit yazısı yazılır.

Sayfa numarası

Madde 25 — Sayfa numarası, yazı alanının sağ altına toplam sayfa sayısının kaçıncısı olduğunu gösterecek şekilde verilir (Örnek: 1/9, 2/7, 5/32).

Aslına uygunluk onayı

Madde 26 — Bir yazıdan örnek çıkartılması gerekiyorsa örneğinin uygun bir yerine "Aslının aynıdır" ifadesi yazılarak imzalanır ve mühürlenir.

Kurum ve kuruluşlar elektronik ortamdaki belgelerin değiştirilmesini ve aslına uygun olmayan biçimde çoğaltılmasını önleyen teknik tedbirleri alır.

DÖRDÜNCÜ BÖLÜM
Resmî Yazıların Gönderiliş ve Alınışlarında Yapılacak İşlemler

Kayıt kaşesi

Madde 27 — Gelen evrak, Örnek 13'te yer alan kayıt kaşesi kullanılarak kaydedilir. Kamu kurum ve kuruluşları Örnek 13'te yer alan kaşeyi örnek alarak kendilerine uygun bir kaşe hazırlar ve kullanırlar. Bu kaşeler evrakın arka yüzüne basıldıktan sonra evrakın tarih ve sayısı yazılır, ünite içinde hangi bölümü ilgilendiriyorsa o bölümün karşısına gereği yapılmak veya bilgi vermek maksadıyla (x) işareti konulur. Ek olduğunda bunların adedi en alt sütunda rakamla belirtilir.

Elektronik ortamda yapılan yazışmalarda, doğrulama yapıldıktan sonra yazı ilgili birime gönderilir.

Yazıların gönderilmesi

Madde 28 — Yazıyı gönderenin iletişim bilgileri zarfın sol üst köşesinde, yazının gideceği yerin iletişim bilgileri ise zarfın ortasında yer alır. Yazının gizlilik derecesi zarfın üst ve alt ortasına, ivedilik derecesi ise sağ üst köşeye gelecek biçimde kırmızı renkle belirtilir.

Çok gizli yazılar çift zarf ile gönderilir. İç zarfa yazı konulur, zarfın kapanma yerlerine hazırlayanın parafları atılır ve saydam bant ile paraflar örtülecek şekilde zarf kapatılır. İç zarfın üzerine de iletişim bilgileri yazılarak, yazının çok gizli olduğu zarfın üst ve alt ortasına, varsa ivedilik derecesi sağ üst köşeye gelecek biçimde kırmızı renkle belirtilir.

İç zarf ve Örnek 14'te gösterilen iki suret evrak senedi dış zarfın içine konularak gizlilik derecesi olmayan yazılar gibi kapatılıp, üzerine gideceği yer ve evrak sayısı yazılır. Dış zarfın üzerinde gizlilik derecesi bulunmaz, varsa ivedilik derecesi kırmızı renkli olarak belirtilir.

Elektronik ortamdaki yazışmalar kurum ve kuruluşların e-posta adresi üzerinden yapılır.

Elektronik ortamda yapılan yazışmaların ve gönderilen belgelerin gizli olması durumunda bunlar bir iletinin ekinde gönderilir ve iletinin konu kısmına gizlilik derecesi yazılır.

"Çok gizli" gizlilik dereceli yazıların alınması

Madde 29 — "Çok gizli" gizlilik dereceli yazılarda, dış zarfı açan görevli iç zarf üzerinde yer alan "çok gizli" ibaresini gördüğünde zarfı açmadan yetkili makama sunar. Bu görevli dış zarfın içinde yer alan evrak senedini imzalayarak bir nüshasını gönderen makama iade eder.

BEŞİNCİ BÖLÜM
Son Hükümler

Yürürlük

Madde 30 — Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

Madde 31— Bu Yönetmelik hükümlerini Bakanlar Kurulu yürütür.

ÖRNEK: 1-BAŞLIK

T.C.
BAŞBAKANLIK
İdareyi Geliştirme Başkanlığı

T.C.
BAŞBAKANLIK
Devlet Personel Başkanlığı

T.C.
GAZİOSMANPAŞA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Kütüphane ve Dokümantasyon Dairesi Başkanlığı

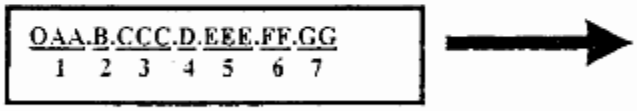
T.C.
ANKARA VALİLİĞİ
İl Sağlık Müdürlüğü

T.C.
BORÇKA KAYMAKAMLIĞI
İlçe Milli Eğitim Müdürlüğü

T.C.
BAYINDIRLIK VE İSKAN BAKANLIĞI
Karayolları Genel Müdürlüğü 4. Bölge Müdürlüğü

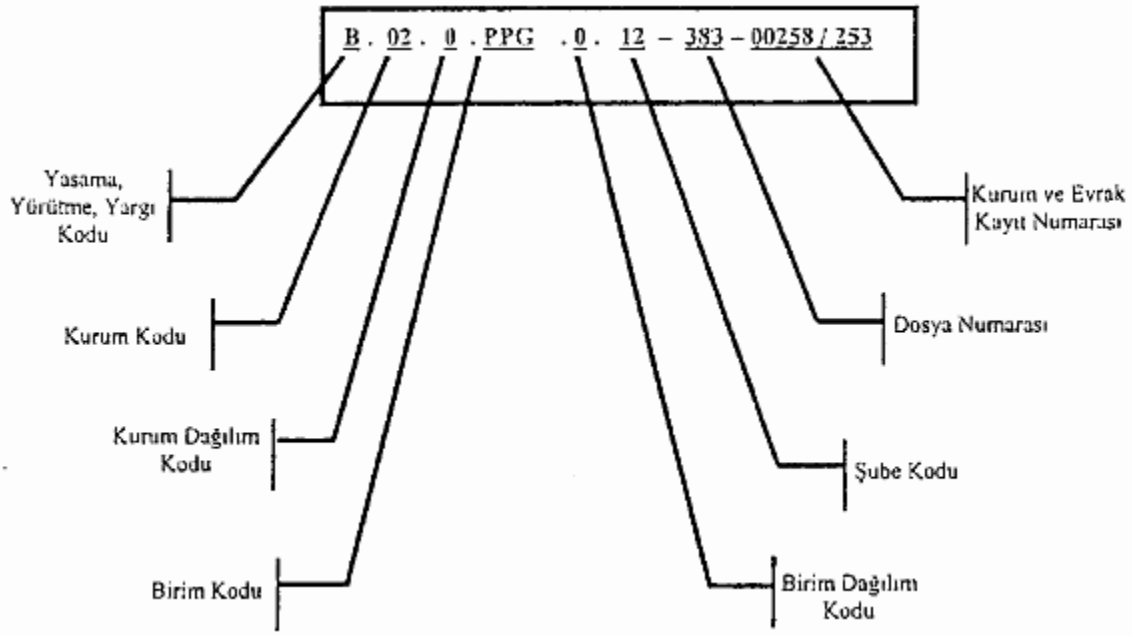
ÖRNEK: 2- SAYI

Sayı: B.02.0.İGB-16-717-752/89
Sayı: B.02.2.TCZ-21-932/467
Sayı: B.08.4.MEM.202-148-694/253



1.Bölüm: Kurum Kodu
2. Bölüm: Kurum Dağılım Kodu
3. Bölüm: Birim Kodu
4. Bölüm: Birim Dağılım Kodu
5. Bölüm: Alt Birim Kodu
6. Bölüm: Ayrıntılı Alt Birim Kodu
7. Bölüm: Alt Tali (Şube) Kodu

YAZIŞMALARDAKİ KOD DAĞILIMI



ÖRNEK: 3-GÖNDERİLEN MAKAM

İÇİŞLERİ BAKANLIĞINA
(Mahalli İdareler Genel Müdürlüğü)

ANKARA VALİLİĞİNE
(İl Milli Eğitim Müdürlüğü)

TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ BAŞKANLIĞINA

Sayın Prof. Dr. Recep TOPARLI
Türk Dil Kurumu Başkan Danışmanı

ÖRNEK: 4-İLGİ

İlgi: a) 13/04/2004 tarihli ve B.02.0.İGB.542/263 sayılı yazı,
b) 28/09/2004 tarihli ve B.02.0.DİB.482-03/281 sayılı yazı,
c) 30/09/2004 tarihli ve B.05.0.PGM.0.06.00.02-03-9804 sayılı yazı.

ÖRNEK: 5-A SAYFA DÜZENİ

GİZLİLİK DERECESİ

T.C.
BAŞBAKANLIK
İdareyi Geliştirme Başkanlığı
İki satır aralığı

İVEDİ
15/07/2004

Sayı :.....

Konu :.....
.....

İki-dört satır aralığı

..... BAKANLIĞINA

İki satır aralığı

İlgi : a) .....
.....
b) .....

İki satır aralığı

.....
.....
.....
.....
.....
.....
.....

İki- dört satır aralığı

(İmza)
Adı Soyadı
Başbakan a.
Müsteşar

Uygun satır aralığı

EKLER :
1- Yazı örneği (....sayfa)
2- Yönetmelik (....sayfa)

Uygun satır aralığı

DAĞITIM:
Gereği:
.....
.....

Bilgi:
.....
.....

GİZLİLİK DERECESİ

Meşrutiyet Cad. 24/5-6 Yenişehir 06640 ANKARA Ayrıntılı bilgi için irtibat: H. KARA Uzman
Telefon: (0 312) 419 97 26 Faks: (0 312) 418 81 90
e-posta: idare@basbakanlik.gov.tr Elektronik Ağ: www.basbakanlik.gov.tr

ÖRNEK: 5-B SAYFA DÜZENİ

GİZLİLİK DERECESİ

T.C.
BAŞBAKANLIK
İdareyi Geliştirme Başkanlığı

İki satır aralığı

İVEDİ
15/07/2004

Sayı :.....

Konu :.....
.....

İki-dört satır aralığı

..... BAKANLIĞINA

İki satır aralığı

İlgi : a) .....
.....
b) .....

İki satır aralığı

.....
.....
.....

Bir satır aralığı

.....
.....
.....

İki- dört satır aralığı

(İmza)
Adı Soyadı
Başbakan a.
Müsteşar

Uygun satır aralığı

EKLER :
1- Yazı örneği (....sayfa)
2- Yönetmelik (....sayfa)

Uygun satır aralığı

DAĞITIM:
Gereği: Bilgi:
....
....

GİZLİLİK DERECESİ

Meşrutiyet Cad. 24/5-6 Yenişehir 06640 ANKARA Ayrıntılı bilgi için irtibat: H. KARA Uzman
Telefon: (0 312) 419 97 26 Faks: (0 312) 418 81 90
e-posta: idare@basbakanlik.gov.tr Elektronik Ağ: www.basbakanlik.gov.tr

ÖRNEK: 6 İMZA

ÖRNEK: 6-A

İmza
Adı Soyadı
Başbakan a.
Müsteşar

İmza
Adı Soyadı
Vali a.
Vali Yardımcısı

İmza
Adı Soyadı
Başbakan V.

ÖRNEK: 6-B

İmza
Adı Soyadı
Genel Müdür Yardımcısı

İmza
Adı Soyadı
Genel Müdür

ÖRNEK: 6-C

İmza
Adı Soyadı
Genel Müdür

İmza
Adı Soyadı
Genel Müdür Yardımcısı

İmza
Adı Soyadı
Daire Başkanı

ÖRNEK: 6-D
(Atama Kararnameleri)

CUMHURBAŞKANI

Başbakan

Bakan

ÖRNEK: 7-A ONAY

..... MAKAMINA

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

İmza
Adı Soyadı
Personel ve Eğitim Daire Başkanı

O L U R
02/07/2004

(İmza)

Adı Soyadı
Genel Müdür

ÖRNEK: 7-B ONAY

..... MAKAMINA

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

İmza
Adı Soyadı
İdareyi Geliştirme Başkanı

Uygun görüşle arz ederim.
01/07/ 2004

(İmza)

Adı Soyadı
Müsteşar Yardımcısı

O L U R
02/07/2004

(İmza)

Adı Soyadı
Başbakan a.
Müsteşar

ÖRNEK: 8-EKLER

EKLER:
1- Yazı örneği (... sayfa)
2- Yönetmelik (... sayfa)

EKLER:
1- Rapor (... sayfa)
2- Disket (… adet)

DAĞITIM:
Adalet Bakanlığına
İçişleri Bakanlığına (Ek-1 konulmadı)
Dışişleri Bakanlığına (Ek konulmadı)
Ulaştırma Bakanlığına (Ek-2 konuldu)

ÖRNEK: 9-DAĞITIM

ÖRNEK: 9-A

DAĞITIM:
Gereği:
Başbakanlığa

Bilgi:
Cumhurbaşkanlığı Genel Sekreterliğine

ÖRNEK: 9-B

DAĞITIM:
81 İl Valiliğine

ÖRNEK: 10-PARAF

08/09/2004	Uzman	: H. ÇELİK (Paraf)
08/09/2004	D. Bşk.	: İ. GÜNAY (Paraf)
08/09/2004	Gn. Md.	: Ö. DEMİR (Paraf)
08/09/2004	Müst. Yrd.	: Y. ARSLAN (Paraf)
08/09/2004	Müsteşar	: İ. ÇETİNKAYA (Paraf)

Meşrutiyet Cad. 24/5-6 Yenişehir 06640 ANKARA Ayrıntılı bilgi için irtibat: H. ÇELİK Uzman
Telefon: (0 312) 419 97 26 Faks: (0 312) 418 81 90
e-posta: idare@basbakanlik.gov.tr Elektronik Ağ: www.basbakanlik.gov.tr

ÖRNEK: 11-KOORDİNASYON

08/09/2004 Uzman : H. KARA (Paraf)
08/09/2004 İd. Geliş. Bşk. : H. KÖKSAL (Paraf)
08/09/2004 Müst. Yrd. : N.ÇAKMAK (Paraf)

Koordinasyon:
08/09/2004 Huk. Müş. : A. USTA (Paraf)
08/09/2004 Müst. Yrd. : N. ÖZCAN (Paraf)

Meşrutiyet Cad. 24/5-6 Yenişehir 06640 ANKARA Ayrıntılı bilgi için irtibat: H. KARA Uzman
Telefon: (0 312) 419 97 26 Faks: (0 312) 418 81 90
e-posta: idare@basbakanlik.gov.tr Elektronik Ağ: www.basbakanlik.gov.tr

ÖRNEK: 12-ADRES

Meşrutiyet Cad. 24/5-6 Yenişehir 06640 ANKARA Ayrıntılı bilgi için irtibat: H. KARA Uzman
Telefon: (0 312) 419 97 26 Faks: (0 312) 418 81 90
e-posta: idare@basbakanlik.gov.tr Elektronik Ağ: www.basbakanlik.gov.tr

ÖRNEK: 13-KAYIT KAŞESİ

Bakanlıklar ile Bağlı ve İlgili Kuruluşların Merkez Teşkilatında

BAKANLIK	Gereği	Bilgi
MÜSTEŞAR		
Birim		
"		
"		
MÜSTEŞAR YARDIMCILIĞI		
Birim		
"		
"		
MÜSTEŞAR YARDIMCILIĞI		
"		
"		
MÜSTEŞAR YARDIMCILIĞI		
"		
"		
EKLER		
KAYIT	TARİH	
	SAYI	

Taşra Teşkilatında

İZMİR VALİLİĞİ İl Millî Eğitim Müdürlüğü		
KAYIT	TARİH	
	SAYI	
HAVALE	GEREĞİ	
	BİLGİ	
DOSYA NO		
EKLER		

ÖRNEK: 14- KONTROLLÜ EVRAK SENEDİ

GÖNDEREN	ALAN	TARİH	SENEDİ HAZIRLAYAN		
Sıra No	Belgenin Konusu (Tarih ve Sayısı)	Kopya Adedi	Kopya No	Ekler	Dil
SENEDİ İADE EDENİN: Adı ve Soyadı : Görevi : İmzası :		Tarih Saat			

27 Ocak 2005 tarih, 205709 sayılı Resmi Gazete **EK-E**

Tebliğ

Devlet Bakanlığından:

Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları

A- SİGORTANIN KAPSAMI

A.1- Sigortanın Konusu

Bu sigorta ile; ulusal veya uluslararası düzeyde nitelikli elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan Elektronik Sertifika Hizmet Sağlayıcısının (ESHS) Elektronik îmza Kanunundan doğan yükümlülüklerini yerine getirmemesi sonucu oluşan, nitelikli elektronik sertifika sahibi kişi veya kuruluşların ve üçüncü şahısların uğrayacağı zararlara ilişkin sorumluluğu, sözleşmede belirlenen zorunlu sigorta limitlerine kadar teminat altına alınmıştır.

Bu sigorta, sigortalıya karşı yapılan talepler sonucundaki yasal giderler için de teminat verir.

A.2- Sigorta Teminatının Kapsamı

Sertifika Mali Sorumluluk Sigortası;

A.2.1. 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,

A.2.2. Sertifikaların içeriğinde ESHS'den kaynaklanan yanlış bilgilerin bulunması,

A.2.3. Sertifikaların oluşturulması sırasında nitelikli elektronik imza sahiplerinin verdikleri bilgilerin ESHS tarafından eksik veya yanlış işlenmesi sonucu ortaya çıkan hataların bulunması,

A.2.4. Sertifikaların ESHS ile nitelikli elektronik imza 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.

Türkiye'de faaliyette bulunan ESHS'nin sigortacının bilgisi dahilinde olan yabancı bir ülkede kurulu başka bir ESHS'ye ait kabul ettiği sertifikalardan doğan maddi zararlar da kapsam dahilindedir.

A.3- Sigorta Sözleşmesinin Süresi

Sözleşmenin süresi taraflar arasında serbestçe belirlenir. Poliçede başlama ve sona erme tarihlerinin gün ve saat olarak yazılması gerekir.

A.4- Teminat Dışında Kalan Haller

Aşağıdaki hallerden birinin veya birkaçının sonucunda doğan sorumluluğa bağlı olarak;

A.4.1. Savaş, düşman hareketleri, çarpışma (savaş ilan edilmiş olsun veya olmasın), ihtilal, ayaklanma ve bunların gerektirdiği inzibati askeri hareketlerden,

A.4.2. 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,

A.4.3. Deprem, yanardağ püskürmesi, deniz depremi, sel, seylap ve su baskını, yer kayması gibi doğal afetlerden,

A.4.4. Kamu otoritesi tarafından yapılacak tasarruflar sonucunda oluşan ve ESHS'nin kusurundan kaynaklanmayan sorunlardan,

A.4.5. İletişim altyapısı ve ESHS'nin doğrudan kontrolü altında olmayan bilgi işlem altyapısında meydana gelen sorunlardan,

A.4.6. İmza sahibi tarafından kanun dışı amaçlar için nitelikli elektronik imzanın kullanılmasından,

A.4.7. 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,

A.4.8. Faaliyet konusu ile ilgili kanun, yönetmelik ve tebliğlerle belirlenen esaslar ve teknik standartlara bağlı kalınmamasından,

doğan zararlar sigorta teminatı dışındadır.

B- ZARAR VE TAZMİNAT

B.l- Rizikonun Gerçekleşmesi

ESHS'nin, sözleşme süresi içinde Kanundan kaynaklanan yükümlülüklerini yerine getirmemesi nedeniyle, sertifika sahibi veya üçüncü kişilerin sözleşme dönemi içinde veya sonrasında zarara uğraması sonucunda;

B.1.1. Sigortacının bilgisi dahilinde olmak koşuluyla sigortalı tarafından ödeme yapılması veya,

B.l.2. Zararın gerçekleştiğinin ve bu zararın ESHS'nin sorumluluğundan kaynaklandığının mahkeme tarafından karar altına alınması veya

B.1.3. Sigortalının tebligat üzerine davayı öğrendiği tarihte,

riziko gerçekleşmiş olur.

B.1.2- Rizikoya İlişkin Olarak Sigorta Ettirenin ve Sigortalının Yükümlülükleri

Sigortalı/sigorta ettiren rizikonun gerçekleşmesi halinde, aşağıdaki hususları yerine getirmekle yükümlüdür:

a) Bu sözleşmeye göre, sorumluluğunu gerektirecek bir olayı, haberdar olduğu andan itibaren beş gün içinde sigortacıya ihbar etmek,

b) Sigortalı değilmişçesine gerekli kurtarma ve koruma önlemlerini almak ve bu amaçla
sigortacı tarafından verilecek makul talimatlara uymak,

c) Sigortacının talebi üzerine, olayın ve zararın nedeni ile hangi hal ve şartlar altında
gerçekleştiğini ve sonuçlarını tespiti, tazminat yükümlülüğü ve miktarı ile rücu hakkının kullanılmasına yararlı, elde edilmesi mümkün bilgi ve belgeleri gecikmeksizin vermek,

d) Zarardan dolayı, dava yolu ile veya başka yollarla bir tazminat talebi karşısında kaldığı veya aleyhine cezai kovuşturmaya geçildiği hallerde, durumdan sigortacıyı derhal haberdar etmek ve zarar ziyan talebine ve cezai kovuşturmaya ilişkin olarak almış olduğu ihbarname, davetiye ve benzeri tüm belgeleri derhal sigortacıya vermek,

e) Sigorta konusu ile ilgili başka sigorta sözleşmesi varsa bunları sigortacıya bildirmek.

B.3- Tazminat ve Ödenmesi

Rizikonun gerçekleşmesi halinde, özel durumlar hariç olmak üzere, hangi belgelerin istenileceği poliçe ekinde yer almak zorundadır. Sigortacı, talep edilen tazminat ve giderleri, hak sahibinin tazminata konu olay ve zarara ilişkin tespit tutanağını veya bilirkişi raporunu ve poliçe ekinde de yer alan diğer gerekli belgeleri eksiksiz olarak şirketin merkez veya kuruluşlarına ilettiği tarihten itibaren on iş günü içinde gerekli incelemeleri tamamlayıp sözleşmeye aykırı olmayan maddi zararlara ilişkin tazminatı öder.

B.4- Halefiyet

Sigortacı, ödediği tazminat tutarınca, hukuken sigortalının yerine geçer.

C- ÇEŞİTLİ HÜKÜMLER

C.l- Sigorta Priminin Ödenmesi ve Sigortacının Sorumluluğunun Başlaması

Sigortacının sorumluluğu, primin tamamının veya taksitle ödenmesi kararlaştırılmış ise ilk taksidin poliçenin tesliminde ödenmesi ile başlar. Aksi

kararlaştırılmadıkça, primin tamamının veya ilk taksidin ödenmemesi halinde, poliçe teslim edilmiş olsa dahi sigortacının sorumluluğu başlamaz ve bu şart poliçeye yazılır.

Prim ödemede temerrüde düşülmesi halinde Borçlar Kanunu hükümleri uygulanır.

C.2- Sigortalının/Sigorta Ettirenin Sözleşme Yapıldığı Sırada Beyan Yükümlülüğü

C.2.1. Sigortacı sigorta sözleşmesini, sigorta ettirenin veya sigortalının beyanı ve varsa teklifname ve eklerinde yazılı sorulara verdiği cevaplara dayanarak yapar.

C.2.2. Sigortalının/sigorta ettirenin beyanı yanlış veya eksik ise ve bu durum, sigortacının sözleşmeyi yapmaması veya daha ağır şartlarla yapmasına neden oluyorsa, sigortacı durumu öğrendiği tarihten itibaren bir ay içinde sözleşmeden cayabilir veya sözleşmeyi yürürlükte tutarak aynı süre içinde prim farkını talep edebilir.

C.2.3. Sigorta ettiren, talep edilen prim farkını kabul ettiğini sekiz gün içinde bildirmediği takdirde sözleşmeden cayılmış olur. Ancak, prim farkının kabul edilmemesi nedeniyle sözleşmeden cayılması, sigortacının gerçeğe aykırı veya eksik beyanı öğrendiği tarihten itibaren bir aylık süre içinde gerçekleşmek durumundadır.

C.2.4 Sigortalının/sigorta ettirenin kasıtlı davrandığının anlaşılması halinde sigortacı, sözleşmeden cayabilir ve gün esasına dayanarak hesap edilen prime hak kazanır.

C.3 Sözleşmenin Devamı Sırasındaki Beyan Yükümlülüğü

Sözleşmenin devamı sırasında sigortacının izni olmadan rizikoya etki edici nitelikte değişiklik yapılması halinde sigorta ettiren veya sigortalı durumu sekiz gün içinde sigortacıya bildirmekle yükümlüdür.

Durumun sigortacı tarafından öğrenilmesinden sonra, değişiklik, sigortacının sözleşmeyi yapmamasını veya daha ağır şartlarla yapmasını gerektiren hallerde ise sigortacı, sekiz gün içinde sözleşmeyi fesheder veya prim farkını talep etmek suretiyle sözleşmeyi yürürlükte tutar. Sigorta ettiren, talep edilen prim farkını kabul ettiğini sekiz gün içinde bildirmediği takdirde sözleşme feshedilmiş olur.

Feshin hüküm ifade ettiği tarihe kadar geçen sürenin primi, gün esası üzerinden hesap edilir ve fazlası geri verilir.

Süresinde kullanılmayan fesih veya prim farkını talep etme hakkı düşer.

Rizikodaki değişikliği öğrenen sigortacı, sigorta hükmünün devamına razı olduğunu gösteren bir harekette bulunursa fesih ve prim talep hakkı düşer.

Değişiklik, rizikoyu hafifletici nitelikte ve daha az prim uygulamasını gerektirir hallerden ise: Sigortacı, bu değişikliğin yapıldığı tarihten sözleşmenin sona ermesine kadar geçecek süre için gün esasına göre hesap edilecek prim farkını sigorta ettirene geri verir.

Sigortacının sözleşmeyi bu değişiklere göre yapmamasını veya daha ağır şartlarla yapmasını gerektiren hallerde:

a) Sigortacı durumu öğrenmeden önce,

b) Sigortacının fesih ihbarında bulunabileceği süre içinde,

c) Fesih ihbarının hüküm ifade etmesi için geçecek süre içinde,

riziko gerçekleşirse, sigortacı, tazminatı tahakkuk ettirilen prim arasındaki orana göre öder.

C.4. Sözleşmenin Devamı Sırasındaki Koruma Yükümlülüğü

C.4.1 Sigortalı, sertifikaları imzalama amacıyla kullandığı imza oluşturma verisini korumaya ilişkin bütün işlemleri, sözleşme süresi boyunca, rizikonun tutarı ve süresini de dikkate alarak, sigortalı değilmişçesine özenle yürütmekle yükümlüdür.

C.4.2. Sigortalı, sertifikaları imzalama amacıyla kullandığı imza oluşturma verisinin, yetkisiz kullanıma veya benzeri bir güvenlik ihlaline konu olduğunu anladığında hemen sigortacıyı haberdar etmek zorundadır.

C.4.3. Sigorta ettiren sigorta ettirdiği sorumluluğuna ilişkin herhangi bir güvenlik ihlalini haber alır almaz, gerekli önlemleri aldıktan sonra, sigortacıya haber vermek zorundadır.

C-5 Sigortalının (ESHS) Değişmesi

Aksine sözleşme yoksa sözleşme süresi içinde sigortalının değişmesi halinde sözleşme yeni sigortalı ile devam eder.

C-6 Birden Çok Sigorta

Sigorta ettiren ya da sigortalı başka sigorta şirketleriyle aynı rizikolara karşı aynı süreye rastlayan başka sigorta sözleşmesi yapacak olursa bunu sigortacılara derhal bildirmekle yükümlüdür.

C.7- Tebliğ ve İhbarlar

C.7.1 Sigortalının/sigorta ettirenin bildirimleri, sigorta şirketinin merkezine veya sigorta sözleşmesine aracılık eden acenteye yapılır.

C.7.2 Sigortacının bildirimleri de sigortalının/sigorta ettirenin poliçede gösterilen adresine veya bu adres değişmişse son bildirilen adresine noter eliyle veya taahhütlü mektupla yapılır.

C.7.3 Taraflara imza karşılığı elden verilen mektup veya telgrafla yapılan bildirimler de taahhütlü mektup hükmündedir.

C.7.4 Güvenli elektronik imza kullanılarak elektronik ortamda yapılan ve sigortalıya/sigorta ettirene ulaştığı kanıtlanabilen bildirimler de geçerli sayılır.

C.8- Ticari ve Mesleki Sırların Saklı Tutulması

Sigortacı ve sigortacı adına hareket edenler bu sözleşmenin yapılması dolayısıyla sigortalıya/sigorta ettirene ilişkin öğreneceği ticari, teknik ve mesleki sırların

saklı tutulmamasından doğacak zararlardan sorumludurlar.

C.9- Yetkili Mahkeme

Sigorta sözleşmesinden doğan anlaşmazlıklar nedeniyle sigortacı aleyhine açılacak davalarda yetkili mahkeme, sigorta şirketinin merkezinin veya sigorta sözleşmesine aracılık yapan acentenin ikametgahının bulunduğu yerdeki, sigortalı/sigorta ettiren aleyhine açılacak davalarda ise davalının ikametgahının bulunduğu yerdeki ticaret davalarına bakmakla görevli mahkemedir.

CIO- Zaman aşımı

Sigorta sözleşmesinden doğan bütün talepler iki yılda zaman aşımına uğrar.

C.II- Özel Şartlar

Sigorta sözleşmesine, sigortalının / sigorta ettirenin aleyhine olmamak kaydıyla özel şartlar konulabilir.

C.12- Yürürlük

Bu Genel Şartlar yayımı tarihinde yürürlüğe girer.

27 Ocak 2005 tarih, 25709 sayılı Resmi Gazete **EK-F**

Tebliğ

Devlet Bakanlığından:

Sertifika Mali Sorumluluk Sigortası
Tarife ve Talimatı

23 Ocak 2004 tarihli ve 25355 sayılı Resmî Gazete'de yayımlanan 5070 sayılı Elektronik İmza Kanunu ve 26 Ağustos 2004 tarihli Resmî Gazetede yayımlanan Sertifika Mali Sorumluluk Sigortası Yönetmeliğine göre yapılacak "Sertifika Mali Sorumluluk Sigortası"na aşağıdaki tarife ve talimat uygulanır.

Türkiye'de kaza branşında ruhsatı olan bütün sigorta şirketleri, Sertifika Mali Sorumluluk sigortasını yapmakla yükümlüdür.

A. TARİFE

Teminat tutarları, sigorta teminatı kapsamına giren olay başına, aşağıdaki şekilde belirlenmiştir:

a) Olay başına : 10.000 YTL.

b) Sözleşme süresince toplam : 1.000.000. YTL.

Sigorta primleri, sigorta şirketlerince serbestçe belirlenir.

Bu Tarife ve Talimatın yürürlüğe girmesinden sonra yapılacak sigorta sözleşmeleri, yukarıdaki teminatlar üzerinden yapılır. Ancak, sözleşme süresi içinde, Hazine Müsteşarlığının bağlı bulunduğu Bakan tarafından teminat tutarları artırıldığı takdirde, eski teminat tutarları üzerinden sigortası yapılmış ve süresi devam eden sigorta sözleşmesine Elektronik Sertifika Hizmet Sağlayıcıları, sigorta şirketlerine başvurarak yeni teminatlar üzerinden Sertifika Mali Sorumluluk Sigortası zeyilnamelerini bu Tarife ve Talimatın yürürlük tarihinden itibaren 15 gün içinde almak zorundadır. Zeyilname yapılmayan ve teminatları yeni limitlere getirilmeyen sigorta sözleşmelerinde, sigorta şirketlerinin sorumluluğu eski teminat tutarları ile sınırlıdır.

Sigorta sözleşmesine bağlı olarak sigorta ettirene yüklenmiş veya yüklenecek vergi, resim, harç ve diğer yükümlülükler sigorta ettirenden alınır.

B. TALİMAT

Bu sigorta, 5070 sayılı Elektronik İmza Kanunu kapsamında Elektronik Sertifika Hizmet Sağlayıcısından nitelikli elektronik sertifika, zaman damgası, elektronik imza hizmetlerinden. birini veya birkaçım alan nitelikli elektronik sertifika sahipleri ve bu sertifikalara dayanarak işlem yapan üçüncü kişileri, Sertifika Mali Sorumluluk Sigortası Genel Şartları'nın 2 nci maddesinde yer alan risklere karşı teminat altına alır.

Elektronik Sertifika Hizmet Sağlayıcısı, şirket merkezi ile internet adresindeki sayfasına sigorta sözleşmesine ait kısa bilgiler ile sigortacının adı ve açık adresini belirten ibareleri kolaylıkla görülebilecek bir yerde bulundurmak zorundadır.

C. YÜRÜRLÜK

Bu Tarife ve Talimat yayımı tarihinde yürürlüğe girer.

KAYNAKÇA

(Brink, 2001) Derek Brink ve diğerleri, "PKI Interoperability Framework", PKIforum white paper

(Entrust, 2000) "The Concept of Trust in Network Security", Entrust Security Digital Identities&Information

(Kiran, 2002) Shashi Kiran ve diğerleri, "PKI Basics-A Technical Perspective", PKIforum PKInote

(Lloyd, 2001) Steve Lloyd ve diğerleri, "CA-CA Interoperability", PKIforum white paper.

(Turnbull, 2000) Jim Turnbull, "Cross-Certification and PKI Policy Networking", Entrust Securing Digital Identities&Information

(Wilson, 2001) Stephen Wilson, "Leveraging External Accreditation to Achieve PKI Cross-Recognition", PricewaterhouseCoopers beTRUSTed

(2005) TÜBİTAK UEKAE KSM web sitesi www.kamusm.gov.tr

Özgür Deniz Erzincan, 15/07/2004 Telekom Dünyası, E-imza ve E-Türkiye Ankara TK e-imza ulusal koordinasyon kurulu altyapı çalışma grubu ilerleme raporu