E-İMZA ULUSAL KOORDİNASYON KURULU
BİLGİ GÜVENLİĞİ VE STANDARTLAR ÇALIŞMA GRUBU
İLERLEME RAPORU

1 YÖNETİCİ ÖZETİ

5070 sayılı Elektronik İmza Kanunu 23.01.2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Sözkonusu Kanunun Yönetmelik başlıklı 20 nci maddesi "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." hükmü ile Telekomünikasyon Kurumunu yetkili kılmıştır.

Ülkemizde elektronik imzanın uygulanmasına ilişkin çalışmaların başlatılmasını teminen 08.03.2004 yapılan toplantı sonrasında oluşturulan 3 çalışma grubundan bir tanesi olan Bilgi Güvenliği ve Standardlar Çalışma Grubu faaliyetleri çerçevesinde, 28 Nisan tarihinde, çalışma grubu başkanı, başkan yardımcısı ve raportörü ile Telekomünikasyon Kurumu ve TSE'den uzmanların katıldığı bir ön toplantı yapılarak taslak raporun oluşumuna kadar gerçekleşecek sürecin yol haritası belirlenmiş ve bu yol haritasına göre 12 Mayıs 2004 tarihinde yapılan çalışma grubu 1. Toplantısında, Telekomünikasyon Kurumu tarafından oluşturulan rapor formatında yeralan maddeler toplantıya katılan kurum temsilcileri arasında paylaştırılmıştır. Raporda; e-imza sahiplerinin sistemi kesintisiz ve güvenli kullanabilmesi ve sertifika hizmet sağlayıcılarının faaliyetlerinin sürekliliği ile uluslararası veya yerli sertifika hizmet sağlayıcılarından alınmış sertifikaların sorunsuz kullanılabilmesi için gözönünde bulundurulması gereken temel kriterler ve standardlar incelenerek geliştirilen öneriler aşağıda sunulan ilerleme raporunda belirtilmiştir.

Uluslararası örnekler incelendiğinde açık anahtar altyapısının (PKI) sayısal imza ve doğrulama amaçlı kullanıldığı görülmüştür. Devlette ise temel amaç olarak kağıt dolaşımını sınırlamak, işlerin elektronik ortamlarda verimli ve süratli bir şekilde yürütülmesi ve vatandaşa sunulan hizmetlerde etkinlik ön plana çıkmıştır. Amaç olarak, kağıtsız ofis, bilgi alma ve gönderme, sağlık işlemleri gibi uygulamalarda doğrulama yönü, elektronik ticaret ve finansal konularda ise sayısal imza yönü ön

plana çıkmaktadır. Sunulacak servislere ve yapılacak işe bağlı olarak kurumların iş akış sistemlerinde ve yapılanmalarında önemli oranda değişim gerektirdiği, çok az uygulamanın "tak çalıştır" mantığıyla bağdaşabildiği tesbit edilmiştir. Yine incelemeler, hizmette süreklilik için sertifikasyon makamları arasında eşgüdümü sağlayacak ve kök sertifikasyon makamının gerekliliği, sertifikasyon politikaları ile kişisel bilgilerin korunmasını sağlama yöntemleri ve ölçme tekniklerinin ayrılmaz bir bütün olduğunu göstermiştir.

Sayısal imza uygulamalarının başarısı ve kullanıma ilişkin risklerin azaltılabilmesi için sistem hakkında kullanıcıların (vatandaş, devlet memuru, işadamı vb.) bilinçlendirilmesi için ivedi tanıtım ve bilgilendirme çalışmalarının başlatılmasının yararlı olacağı değerlendirilmiştir.

2 RAPORUN AMACI VE KAPSAMI

Bu raporun amacı; 23.01.2004 tarihinde yayınlanan 5070 sayılı Elektronik İmza Yasasının uygulanmasına yönelik ISO, ETSI, CEN, EESSI gibi uluslararası standartların incelenmesi, Kurum tarafından yapılacak düzenlemelere esas teşkil etmek üzere, nitelikli sertifika sağlayıcılarının fiziksel, personel ve şebeke güvenliklerinin sağlanması ve kullanıcıların elektronik imza uygulamalarını güvenli olarak gerçekleştirebilmesi için uyulması gerekli standartlar ve alınması gerekli tedbirler konusunda öneriler getirilmesidir.

3 RAPORUN HAZIRLANMASINA KATKIDA BULUNANLAR

Bilgi Güvenliği ve Standartlar Çalışma Grubu'nun 100'ü aşkın üyesi bulunmasına rağmen, raporun hazırlanmasına katkıda bulunan ve toplantıya katılan üyelerin sayısı 27 ile sınırlı kalmıştır. Aşağıda toplantıya katılan ve/veya aktif olarak katkıda bulunan üyelerin isimleri yeralmaktadır:

Rasim YILMAZ (TSE, Çalışma Grubu Başkanı)
Hakan YILDIRIM (Emniyet Genel Müdürlüğü)
Önder ÖZDEMİR (TBD, Çalışma Grubu Raportörü)

Tunga GÖKHUN (TSE, Çalışma Grubu Raportörü)
Ibrahim Öztürk (Turkcell A.Ş.)
Yüksel SAMAST (FORSNET)
Doç. Dr. Ahmet Koltuksuz (Izmir Yüksek Teknoloji Enstitüsü)
Murat Lostar (Lostar Bilgi Güvenliği A.Ş.)
Tuncer Üney (Türkiye Bilişim Vakfı)
Deniz GÜVEN (HSBC Direct Banking - Channel Management)
Bilal YILDIRIM (Dış Ticaret Müsteşarlığı)
Arzu TEKİR (BABSPAG Stratejik Planlama Araştırma Geliştirme & Tic. A.Ş.)
Mete KARAR (Sermaye Piyasası Kurulu)
Yücel YILDIZ (Eximbank)
Mehmet ÇELEBİOĞLU (Eximbank)
Tunay DOĞAN (Koç Sistem Bilgi ve İletişim Hizmetleri A.Ş.)
Rukiye KÖSEGİL (Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü)
Evren BİLGİÇ (Emniyet Genel Müdürlüğü BİDB Guvenlik ve Proj. Şube Müd.)
Demet (ÖZTÜRK) KELES (Gümrük Müsteşarlığı)
Orhan SAMAST (FORSNET)
N. Atilla BİLER (TÜBİTAK-BİLTEN)
Ferda TOPCAN (TÜBİTAK-BİLTEN)
Yılmaz ATASOY (Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü)
Semih DOKURER (Emniyet Genel Müdürlüğü Kriminal Polis Lab. Dai.Bşk.)

4 ELEKTRONİK İMZA UYGULAMALARINA İLİŞKİN STANDARTLAR

4.1 AB Ülkelerinin elektronik imzaya ilişkin mevzuatında referans verilen standartlar

- CWA 14167-1 (Mart 2003): Elektronik İmza Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları — Bölüm 1: Sistem Güvenlik İhtiyaçları

- CWA 14167-2 (Mart 2002): Elektronik İmza Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları — Bölüm 2: Sertifika Servis

Sağlayıcıları İmzalama işlemleri için Kriptolama Modülü — Koruma Profili (MCSO-PP)

- CWA 14167-3 (Haziran 2003): Elektronik İmzalar için Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları – Bölüm 3: Sertifika Servis Sağlayıcıları Anahtar Oluşturma Hizmetleri için Kriptolama Modülü – Koruma Profili.

- CWA 14169 (Mart 2002): nitelikli imza oluşturma araçları

- CWA 14355 (Haziran 2002): Güvenli İmza Uygulama Rehberi- Oluşturma Araçları

4.2 5070 Sayılı Kanun Uyarınca Hazırlanacak Yönetmelik(ler)de Dikkate Alınması Gereken Standartlar

Madde 4.1'de belirtilen standardlara ilaveten, güvenlikle ilgili olarak aşağıda verilen standardların da gözönüne alınması gerekmektedir:

TS ISO/IEC 17799 (2002) Bilgi teknolojisi — Bilgi güvenliği yönetimi için uygulama prensipleri

BS 7799-2 (2002) Bilgi Güvenliği Yönetim Sistemleri — Kullanım İçin Özellikler Rehberi

TS ISO/IEC 15408-1 (2002) Bilgi teknolojisi — Güvenlik teknikleri- Bilgi teknolojisi (IT) güvenliği için değerlendirme kriterleri — Bölüm 1: Giriş ve genel model

TS ISO/IEC 15408-2 (2002) Bilgi teknolojisi — Güvenlik teknikleri- Bilgi teknolojisi (IT) güvenliği için değerlendirme kriterleri — Bölüm 2: Güvenlik fonksiyonel gereksinimleri

TS ISO/IEC 15408-3 (2003) Bilgi teknolojisi — Güvenlik teknikleri — Bilgi teknolojisi (IT) güvenliği için değerlendirme kriterleri — Bölüm 3: Güvenlik garanti gereksinimleri

4.2.1 Güvenli elektronik imza oluşturma araçları ile ilgili standartlar

5070 sayılı Kanun'un 6.maddesinde güvenli elektronik imza oluşturma araçlarının aşağıdaki koşulları yerine getirmesi zorunluluğu belirtilmiştir:

- Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmaması,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiç bir biçimde çıkarılamamasını ve gizliliğini sağlaması,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesi, kullanılamaması ve elektronik imzanın sahteciliğe karşı koruması,
- İmzalanacak verinin imza sahibi dışında değiştirilememesi ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesi.

Yukarıda sayılan özelliklerden güvenli elektronik imza oluşturma aracı olarak akıllı kart ya da token ifade edilmiştir. İlgili donanımın özellikleri ve standartlarında BM UNCITRAL (United Nations Commission on International Trade Law-Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu) da belirtilen hususlar ve ilgili standartlar (CEN, ETSI, ISO vb.) değerlendirilmektedir (Sözkonusu standardlarla ilgili incelemeler sürmektedir).

Elektronik imzalar, uygulamalı matematiğin mesajları anlaşılmaz formlara çeviren bölümü yardımıyla kripto yolu ile oluşturulurlar. Elektronik imzada kullanılan anahtarlar, bir kripto algoritması ile üretilir. Sonucun güvenilir olması için bu sürecin belli standartlarla desteklenmesi gerekir.

Avrupa Konseyi ve Avrupa Parlamentosunun 13 Aralık 1999 tarih ve 1999/93/EC sayılı direktifi ile elektronik imza ile ilgili esaslar belirlenmiştir. Ek II - f maddesinde nitelikli sertifika verecek olan sertifika hizmet sağlayıcılarının değişikliklere karşı korunmuş, destekledikleri işlemlerin teknik ve kriptolojik güvenliği garanti edilen güvenilir sistemler ve ürünler kullanmaları şart koşulmuştur. Ayrıca burada yer alan Ek III'e göre, nitelikli imza oluşturma araçları aşağıdaki gereksinimleri sağlamalıdır:

1. Nitelikli imza oluşturma araçları, aşağıdaki koşulları uygun teknik ve yordamsal yöntemlerle garanti etmelidir:

(a) İmza oluşturmak için kullanılan imza oluşturma verisi, pratikte sadece bir kez olabilir ve gizliliği rasyonel olarak garanti edilir.

(b) İmza oluşturmak için kullanılan imza oluşturma verisine, rasyonel olarak ulaşılamayacağı garanti edilmelidir ve imza mevcut teknolojileri kullanarak sahtekarlığa karşı korunmalıdır

(c) İmza oluşturmak için kullanılan imza oluşturma verisi, başkalarının kullanımına karşı yasal imza sahibi tarafından güvenilir bir şekilde korunabilmelidir.

2. Nitelikli imza oluşturma araçları imzalanacak veriyi değiştirememeli ya da imzalama süreci öncesi imza sahibine verinin sunulmasını önleyememelidir.

Avrupa Elektronik İmza Standardizasyonu, ICT Standart Yönetimi (The ICT Standards Board, CEN, ETSI ve CENELEC Avrupa standart organizasyonlarının işbirliğinde oluşturulan bir inisiyatiftir) tarafından Avrupa Komisyonu direktifleri sonucunda ele alınmıştır. Elektronik imza oluşturma araçlarının işlevsel ve kalite standartlarında olması gerekir.

Güvenli imza geliştirme araçlarının,

- Pratikte sadece bir kez üretilebilirliğe
- Gizliliğe,
- Yüksek kalitede anahtar üretimine ve anahtar korumasına,
- Güçlü algoritmalara ve yeterli anahtar uzunluğuna,
- PIN/şifre yapısının sözlük ve etkin bitirici ataklara dayanıklı olmasına,
- İmzanın üretildiği araç içerisinden anahtarın hiçbir zaman ayrılamama özelliğine,
- Aracın hiçbir yedek ya da kopya üretilmeme özelliğine

sahip olması gerekmektedir.

Güvenli imza oluşturma süreci bağlamında kullanıcı arayüzü, imzalama öncesi bilginin doğrulanması talebi, PIN'in her zaman girilme zorluğu, imzalama aracının ve PIN'in sertifika servis sağlayıcı ile uyumlu olarak kontrol altında tutulma kriterleri dikkate alınmalıdır.

Güvenli imza oluşturma işletimi ve yönetimi bağlamında ise güvenilir kart okuyucu ve kötü niyetli yazılımlara karşı koruma özelliklerinin esas alınması gerekmektedir.

Avrupa Elektronik İmza Standardizasyon İnisiyatifi bünyesinde yer alan CEN (Avrupa Standardizasyon Teşkilatı) ve ETSI (Avrupa Telekomünikasyon Standart Enstitüsü) Avrupa Bilgi Toplumunun gelişimi için açık, kapsamlı ve esnek bir Avrupa platformu sunmaktadır. 1999/93/EC direktifinin eklerinin ihtiyaçları temelinde elektronik imza standartları (CWA-CEN çalıştay mutabakatı ve ETSI TSETSI teknik spesifikasyonu) geliştirilmiştir.

Avrupa Parlamentosu ve Konseyinin 1999/93/EC direktifine uyumlu olarak 14 Temmuz 2003 tarihinde Konsey tarafından tanımlanmış elektronik imza standartları yayımlanmıştır.

Buna göre Ek'te sunulan listede Üye Devletlerin elektronik imza ürünleri için genel olarak tanımlanmış standartları kabul etmesi belirtilmiştir. Bunlar;

— CWA 14167-1 (Mart 2003): Elektronik İmza Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları — Bölüm 1: Sistem Güvenlik İhtiyaçları

— CWA 14167-2 (Mart 2002): Elektronik İmza Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları — Bölüm 2: Sertifika Servis Sağlayıcıları İmzalama işlemleri için Kriptolama Modülü — Koruma Profili (MCSO-PP)

— CWA 14169 (Mart 2002): nitelikli imza oluşturma araçları.

Daha sonra aşağıdaki standart da yayımlanmıştır.

— CWA 14167-3 (Haziran 2003): Elektronik İmzalar için Güvenilir Sistem Yönetim Sertifikaları için Güvenlik İhtiyaçları – Bölüm 3: Sertifika Servis

Sağlayıcıları Anahtar Oluşturma Hizmetleri için Kriptolama Modülü – Koruma Profili.

Avrupa Parlamentosu ve Konseyi tarafından belirtilen standartların ülkemizde de kullanılması yerinde olacaktır.

4.2.2 Güvenli elektronik imza doğrulama araçları ile ilgili standartlar

ETSI SR 002 176 V1.1.1 (2003-03)
Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

1) Bu raporda e-imzada ve SSCD'de kullanılacak olan kriptografik algoritmalar ile bunlara ilişkin teknik kriterler yer almaktadır.
2) Bu raporda kriptografik algoritmalar için yönetim uygulamaları, imza suite'leri, kriptografik hash fonksiyonları, padding yöntemleri, random sayı üretimi ve imza algoritmaları ile anahtar üretme algoritmalarına ilişkin hususlara yer verilmektedir.
3) Onaylanan imza suite'lerine ilişkin tabloda teknik kriterler ve bu kriterlerin hangi tarihe kadar uygulanacağına ilişkin hususlar bulunmaktadır.
4) RSA, DSA, ECC'ye ilişkin teknik kriterler bulunmaktadır.
5) OID'ye ilişkin teknik kriterleri içeren tablo bulunmaktadır.

ETSI TS 101 903 V1.2.2 (2004-04)
XML Advanced Electronic Signatures (XAdES)

1) XAdES-BES (Basic Electronic Signature), XAdES-EPES (Explicit Policy based ES) ve XAdES-C (ES with Complete Validation Data) olmak üzere 3 farklı XML ileri e-imza formu tanımlanmıştır.
2) Ayrıca XAdES-T (ES with Time), XAdES-A (Archival ES), XAdES-X-L (Extended long ES with time) ve XAdES-X (Extended signatures with time forms) olmak üzere başka XML formatında e-imzalar da tanımlanmıştır.

4.2.3 Elektronik sertifika hizmet sağlayıcısının karşılaması gereken teknik ve idari standartlar

ETSI TS 102 042 V1.1.1 (2002-04)
Policy Requirements for Certification Authorities issuing Public Key Certificates

1) Public Key Certificate veren CA'lara ilişkin olarak uygulanacak olan kural ve politikalar ile hangi tip sertifikaların nasıl ve hangi prosedürle verileceği konusundaki hususları içermektedir.
2) Politika kuralları çerçevesinde Normalized Certificate Policy (NCP), Lightweight Certificate Policy (LCP) ve Extended NCP (NCP+) olmak üzere 3 adet referans sertifika politikası belirlenmiştir. Ancak bu standardı kabul eden CA'lar, burada belirtilen 3 farklı politikadan hangisini uygulayacaklarını açıkça ilan etmelidirler.
3) Sertikasyon hizmetleri, esas itibariyle kayıt, sertifika üretme, dağıtma, iptal yönetimi, iptal durumu bilgileri ve tercihen de sertifika sahibi cihaz tedarik hizmeti olmak üzere 6 farklı konuda hizmet tanımlanmıştır.
4) CP'ler, CPS'lere göre daha kısa ve öz dokümalardır. CA gerektiğinde başka dokümanlar da yayınlayabilir.
5) NCP : Güvenli kullanıcı cihazının (imzalama ya da şifre çözme) kullanımını gerektirmeden 99/93/EC'de belirtilen hukuki kısıtlamalar olmaksızın TS 101 456'da belirtildiği üzere QCP tarafından tavsiye edildiği üzere aynı niteliğe haiz politika.

ETSI ES 201 733 V1.1.3 (2000-05)
Electronic Signature Formats

1) Bu standardda e-imza formatlarına ilaveten Timestamping kurumları gibi Trusted Service Providers'ların işleyişine ilişkin hususlar ve çapraz sertifikalar ile iptal listelerine de yer verilmektedir.
2) Bu standardda timestamping'e yer verilmesinin nedeni, çok uzun süreli olarak şifrelerin kırılması ya da çalınmasına karşılık olarak (compromise) korumanın sağlanması ve kullanılan algoritmaların zamanla kırılamama gücünün azalması sonucu oluşabilecek olumsuzluğu karşı olarak timestamping'in sağlamış olduğu ilave güvenlik yani inkar edememe özelliğinin sağlanması nedeniyledir.
3) Bu standardda ayrıca e-imza token ve imza politikalarına ilişkin formatlara da yer verilmektedir.
4) Bu standard, RFC 2630, X.509, RFC 2459 esas alınarak hazırlanmıştır.

5) E-imza başta imza politikası, imzalanan kullanıcı verisi, sayısal imza ve imza sahibi tarafından sağlanan diğer imza vasıflarını (attributes) içermektedir. Ancak, e-imzayı geçerli kılmak ve doğrulamak için ise gerekli olan ilave data olarak isimlendirilen validation data ise sertifikayı, iptal durum bilgisini ve Trusted Service Provider'den sağlanan timestamp'ı içermektedir.

6) E-imza aşağıda belirtildiği üzere 3 ayrı formatta bulunabilir.

ES (Electronic Signature) : imzalayan tarafından sağlanan temel bilgileri ve sayısal imzayı içerir.

ES-T (ES with Timestamp) : Uzun süre geçerliliğin sağlanması amacıyla ES'e timestamp eklenmiş halidir.

ES-C (ES with Complete validation data) : E-imzanın geçerliliğini sağlayan veri grubu yani iptal durum bilgisinin ilave edildiği ES-T.

7) İmzalayan kişi en azından ES ya da bazı durumlarda ES-T ve çok daha kritik durumlarda ES-C'yi sağlamalıdır. Ancak imzalayan ES-T'yi sağlamazsa verifier, eimzayı aldığında ES-T'yi oluşturmalıdır. Benzer şekilde imzalayan kişi ES-C sağlamazsa verifier, diğer geçerli kılma ve iptal bilgilerine ilişkin veriler mevcut ve hazır olduğunda ES-C'yi oluşturmalıdır. Standardda 14.sayfadaki güzel şekli al.

8) İmza politikası, imzalayanın e-imzasına bağlo olup global olarak tek bir unique referans numarasına sahip olmalıdır.

9) İmza validation policy, ASN.1'e dayalı olarak hazırlanmıştır. İmza doğrulama politikasında TSP'lerin (CA, Attribute Authority, Timestamping Authority) kullanımına ilişkin kuralları içerir.

10) İmza doğrulama politikası, imzalayan tarafından sağlanması gereken bir e-imzanın bileşenlerinin ve bir arbitrator, auditory ya da diğer bağımsız taraflarca daha sonradan ve bir verifier tarafından e-imzanın alıdığında bir e-imzayı doğrulamak için kullanılan ilave diğer bileşenleri (verifier bileşenler) tanımlar.

11) İmzalayan tarafından belirtilen imzanın atıldığı ifade edilen zaman ile bu sertifikada bulunan timestamp herhangi bir uyuşmazlık ve çelişki durumunda bahsedilen bu 2 tarih karşılaştırılır ve aralarında mantıklı bir bağlantının bulunması gerekmektedir. Aradaki fark ise Signature Validation Policy'de belirtilen bir kaç dakika, saat ya da gün cinsinden belirtilerek gerekli doğrulama yapılır.

12) Doğrulama verilerinin esas unsurları olarak iptal durum bilgisi, CRL bilgisi, OCSP bilgisi, sertifikasyon yolu ve timestamping belirlenmiştir.

13) Bu standardın eklerinde şunlar bulunmaktadır.

EK A : ASN.1 X.208'in kullanıldığı imza formatı
EK B : MIME ve örnek yapısal içerikler
EK C : 99/93/EC ve EESSI arasındaki ilişki
EK D : E-imza token'larını oluşturma ve doğrulama için API'lar
EK E : Kriptografik algoritmalar
EK F : Sertifika sahibinin isminin yazılması ve belirlenmesine ilişkin kurallar, pseudonym kuralları

NCP+ : Güvenli kullanıcı cihazının (imzalama ya da şifre çözme) kullanımını gerektiren politika.
LCP : Nispeten daha düşük seviyede kriterleri gerektiren politika.
Sözkonusu 3 ayrı politikaya ilişkin olarak kullanılacak standart gösterimler (Object Identifiers) bu standardda belirlenmiştir.
6) CA ve aboneye verilen yükümlülük ve sorumluluklar maddeler halinde belirtilmiştir.
7) CPS'de asgari bulunması gereken kriterlere yer verilmiştir.

ETSI TS 102 231 V1.1.1 (2003-10)
Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information

1) TSP'lerin hangisinin onaylı ya da geçerli veya faaliyette olduğunun tesbiti için yayınlanan TSL (Trust-service Status List), tercihen on-line olarak ve off-line olarak yayınlanabilir.
2) Bu standardda TSL'ye ilişkin usul ve esaslar yer almaktadır.
3) Sayfa 12'de örnek bir TSL listesi yer almaktadır.
4) EK A : ASN.1'deki uygulama
EK B : XML'deki uygulama

ETSI TS 102 158 V1.1.1 (2003-10)

Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

1) E-ticarette irtibat kurulan kişinin örneğin bir şirketteki müdür gibi pozisyonunun da bilinmesi son derece önemli olup hu husus ya PKC ya da AC (Attribute Certificate) kullanılarak öğrenilebilir.
2) AC'yi AA'lar (Attribute Authority) yayınlar.
3) AC'lerin üretilmesi, dağıtılması, iptal yönetimi ve listesi gibi AC'lere ilişkin usul ve esaslara yer verilmekte ve bu çerçevede AC'lere ilişkin bir politikanın geliştirilmesi gerekmektedir.
4) AA'lar da 99/93/EC'de belirtildiği üzere CSP sayılır.
5) AA'lara ilişkin Attribute Certificate Policy (ACP) ve Attribute Certification Practice Statement'e (ACPS) ilişkin temel hususlara yer verilmektedir.
6) AA'lara ve kullanıcılara ilişkin olarak getirilen yükümlülükler bulunmaktadır.
7) AA'ların anahtar üretimi, yedeklenmesi, yeniden geri kazanımı, güvenlik yönetimi, personel ve fiziki güvenlik hususları yer almaktadır.

ETSI TR 102 044 V1.1.1 (2002-12)
Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates

1) Hizmet sağlayıcının ilgili vasfı bittiğinde, görev veya vekalet sona erdiğinde ilgili sertifika iptal edilir.
2) Bu teknik raporun sonundaki ekte İtalya'da bu konuda kullanılan klavuz doküman bulunmaktadır.

ETSI TS 101 456 V1.2.1 (2002-04)
Policy requirements for Certification Authorities issuing Qualified Certificates

1) Nitelikli sertifika verme hizmeti esas olarak kayıt servisi, sertifika üretme ve dağıtma servisi, iptal yönetimi ve iptal durum bilgisi servisi ve imza sahibi cihazı tedarik servisi olmak üzere çeşitli alt bileşenlerden meydana gelir.

2) QCP'nin tanımı yapılmakla beraber "QCP+SSCD" ve "QCP" olmak üzere 2 çeşit nitelikli sertifika politikası bulunmaktadır. QCP; 99/93/EC'nin EK-1 ve Ek-2'de yer alan şartları sağlayan ve halka verilen sertifikalar için uygulanan politikadır. QCP+SSCD ise, QCP'de gereken kriterlere ilaveten Direktif'in Ek-3'ündeki şartları sağlayan SSCD'nin kullanımı zorunlu tutulmaktadır. Bu 2'si arasındaki tek fark SSCD'nin kullanılmasıdır.
3) CA ve kullanıcıya verilen görev ve yükümlülükler ayrıntılı olarak ele alınmıştır.
4) CPS, anahtar üretimi ve anahtar yaşam yönetimi, saklanması, recovery, yedeklenmesi ve dağıtımına ilişkin temel hususlar verilmektedir.
5) SSCD'nin kullanımına ilişkin hususlar verilmektedir.
6) CA'da güvenlik yönetimi, personel güvenliği, fiziki ve çevre güvenliği, faaliyet yönetimi, sistem erişim yönetimi, CA'nın faaliyetinin sona ermesine ilişkin hususlar bulunmaktadır.

ETSI TR 102 030 V1.1.1 (2002-03)
Provision of harmonized Trust Service Provider status information

1) Güvenen taraflara eğer belirli bir TSP'nin belirli bir hizmetin sunulduğu anda supervision, onay ya da kabul edilmiş başka bir prosedüre uygun olarak çalışıp çalışmadığına ilişkin bilginin sunulması son derece önemlidir. Bu bilgi tercihan on-line olarak sunulması gerekmekte olup off-line olarak da sunulabilir.
2) Güvenen taraf, işlem yaparken TSP tarafından sunulan hizmetin güvenilir olup olmadığını bilmesi son derece önemlidir. Bu da durum bilgisinin tercihan on-line olarak sağlanması ile mümkündür. Burada kullanılan TSP aslında daha genel bir anlam katmak amacıyla 99/93/EC'de belirtilen CSP yerine kullanılmıştır. Ancak işlem yapan taraf işlem yaptığı karşı tarafın temin ettiği hizmet sağlayıcısının güvenilirliğini garanti edemeyeceği için burada hiyerarşik bir sertifika yolunun kurulmuş olması önem arzetmektedir. Bu nedenle bu prosedürde harmonizasyon sağlanmış olmalıdır.
3) Supervision ve voluntary prosedürlerinin AB, EFTA, USA ve Kanada gibi ülkelerde nasıl çalıştığı konusunda açıklamalar bulunmaktadır.
4) Cross-certification, BCA ve hiyerarşi gibi sertifikasyon yöntemlerinin avantaj ve dezavantajları karşılaştırılmaktadır.
5) TSP durum listeleri ve TSL genel yapısına ilişkin açıklamalar bulunmaktadır.

ETSI TR 102 045 V1.1.1 (2003-03)

Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model

1) Bu standardın amacı, farklı imza politikalarını ele alarak TS 101 733 ve TR 102 038'i tamamlamaktır.

2) Direktif gereğince aşağıda belirtildiği üere 7 farklı e-imza tanımlanmıştır.

a) basit e-imza (Madde 5.2)
b) ileri e-imza (Madde 2.2)
c) ileri e-imza + nitelikli sertifika
d) ileri e-imza + PKC + SSCD (ya da SCD)
e) ileri e-imza + nitelikli sertifika + SCD
f) nitelikli e-imza (Madde 5.1)
g) nitelikli e-imza + CA akreditasyonu

3) İmza politikaları, hazırlanması ve bunları hukuki etkileri değerlendirilmektedir.

ETSI TR 102 040 V1.2.1 (2004-02)

International Harmonization of Policy Requirements for CAs issuing Certificates

1) Bu raporda, CA'lar için uygulanacak politika kuralları (ETSI QCP olarak da adlandırılan TS 101 456 ve TS 102 042) hususunda mevcut ETSI TS'i uluslararası tanınmış standartlar ve ilgili faaliyetler ile uyumlaştırmak için yapılan çalışmaların sonuçlarına yer verilmektedir.

2) IETF PKI X.509 (PKIX) çalışma grubunun Certification Policies ve Certification Practices Framework konusunda yayınlamış olduğu RFC 2527 dikkate alınarak ETSI QCP geliştirilmiştir.

3) RFC 2527, IETF tarafından RFC 3647 olarak revize edilmiştir. Bu revizyon, küçük teknik değişiklikler içermekte ancak özellikle sorumluluklar gibi bazı alanlarda özellikle PKI politikası ve practice statements'de önemli değişiklikler getirilmiştir. Bu çerçevede ileride ETSI'de bu değilşiklikleri esas alarak ETSI QCP'de bazı revizyonlar yapabilecektir.

4) Amerikan Baro Birliği (ABA) Bilgi Güvenliği Komitesi (ISC), PAG (PKI Assessment Guidelines) adında yayınladığı doküman ile konu ile ilgili olarak genel hukuki çerçeveyi vermekte olup aynı zamanda 99/93/EC Direktifine ilişkin olarak

küçük bir klavuz da içermektedir. Ayrıca, ABA ISC tarafından hazırlanmakta olan "Model Terms for Certification Services Agreements" dokümanı ETSI'nin TS 101 456 ve TS 102 042 ile de yakından bağlantısı ve benzerlikleri bulunmaktadır.

5) ABD'de hükümet içi ve hükümetler arası güvenli PKI altyapısını kurmak ve işletmek üzere adında başlatılan Federal PKI (FPKI) projesi ile, "Federal Bridge CA CP" geliştirimesi hedeflenmiştir. Bu çerçevede US FPKI ve ETSI ESI yetkililerinden oluşan çalışma grubu RFC 2527'ye dayalı olarak hazırlanmış olan FPKI ve ETSI QCP mapping dokümanı üzerinde çalışılmıştır.

6) Benzer çalışmalar APEC ile de yürütülmektedir.

ETSI TS 101 862 V1.3.1 (2004-03)
Qualified Certificate Profile

1) Direktif'in Madde 5'inde belirtildiği üzere nitelikli sertifikalar öneme haiz olduğundan nitelikli sertifikaya dahip ileri e-imzalar hukuki işlemlerde delil olarak sayılmaktadır.

2) Bu standardda RFC 3739'da belirtilen teknik kriterler esas alınarak nitelikli sertifika profili oluşturulmuştur. Ancak RFC 3739 standardı bilahare RFC 3280 ve daha sonra da X.509 V3 halini almıştır.

3) Sertifikanın nitelikli olduğuna dair bir ibarenin bulunması zorunludur.

4) Sertifikaya getirilen işlem kısıtlamaları ayrıca belirtilebilir, buna ilişkin olarak kullanılacak kodlar ISO 4217'de belirtilmiştir.

4.2.4 Nitelikli elektronik sertifikaların iptal edilmesine ilişkin usul ve esaslar ile bu konuda uygulanmakta olan standartlar

Bu konuda herhangi bir standart olmayıp çeşitli ülkeler tarafından usül ve esaslar belirlenmiştir.

4.2.5 Yabancı elektronik sertifikaların Türkiye'de kurulu sertifika hizmet sağlayıcıları tarafından kabul edilmesi durumunda aranacak standartlar

Aşağıda belirtilen temel dokümanlara uygunluk aranmalıdır.. Ayrıca bir standarda rastlanmamıştır.

FIPS 140-1, 2 Kriptografik modüller için güvenlik gereksinimleri,
FIPS 186-2 Sayısal imza standardı(ABD),
SP 800-25 Sayısal imza ve kimlik denetimi için açık anahtar teknolojisinin federal kurumlarda kullanımı.
SP 800-15 PKI bileşenleri için minimum birlikte çalışabilirlik özellikleri.

4.2.6 Zaman damgası ile ilgili standartlar

ETSI TS 101 861 V1.2.1 (2002-03)
Time Stamping Profile

1) TSP, IETF tarafından RFC 3161'de belirlenmiş olmakla beraber Time Stamping, sayısal izmanın sertifikanın geçerlilik süresi içinde bir dokümana eklenip eklenmediğinin bilinmesi açısından son derece önemlidir.
2) TSP Client tarafında, talep formatında time stamp işlemine tabi tutulacak bilgiyi hash'lemek için kullanılabilecek algoritmalar olarak SHA-1 ya da RIPEMD-160'ın kullanımı önerilmekte ancak cevap formatında ise RSA'lı SHA-1'in kullanılması gerektiği ifade edilmektedir. Ayrıca, RSA algoritması için 1024 ve 2048'in, DSA algoritması için de en az 1024 bit'in desteklenmesi gerektiği ifade edilmektedir.
3) TSP server tarafında ise hash algoritmaları olarak SHA-1, MD5 ya da RIPEMD-160'ın kullanılabileceği ifade edilmektedir. Ayrıca, RSA algoritması için 1024 ve 2048'in desteklenmesi gerekmektedir.
4) Transport protokolleri kısmında ise her TSA için bir adet on-line protokol ve bir adet store and forward protokol desteklenmelidir. RFC 3161'de 4 adet protokol tanımlanmış olmakla beraber HTTP vasıtasıyla Time Stamp Protocol'un desteklenmesi gerektiği ifade edilmektedir.
5) SHA-1 (FIPS Pub. 180-1), MD5 (RFC 1321) ve RIPEMD-160 (ISO/IEC 10118-3)'ün tanımları yapılmıştır.
6) İmza algoritması olarak RSA imza algoritması, RFC 2437'de tanımlanmış olup, RFC 2437'de SHA-1'li RSA imza algoritması ve MD5 mesaj özeti algoritmasının kullanımına ilişkin hususlar yer almaktadır.

ETSI TS 102 023 V1.2.1 (2003-01)

Electronic Signatures and Infrastructures (ESI); Policy requirements for Timestamping Authorities

1) RFC 3161 esas alınarak hazırlanan TS 101 733'de de belirtildiği üzere timestamping'in önemi işlemlerde her geçen gün artmaktadır.

2) Bu standardda TSA'nın (Timestamping Authority) çalışmasına ilişkin usul ve esaslar düzenlenmekle beraber TSA da 99/93/EC gereğince bir nevi CSP sayılmaktadır. (Madde 5.1 ve Madde 2(11))

3) TSU (Timestamping Unit) tarafından sayısal olarak imzalanmış ve UTC ile senkronize olan timestamp token'ları yayınlayan TSA'lar genelde bağımsız kuruluşlardır.

4) Timestamping protokolunun tanımı, RFC 3161 ve TS 101 861'de verilmiştir.

5) Bir TSA birden fazla TSU çalıştırabilir ancak bunların her birisinin farklı anahtarları vardır.

6) TSA'la da diğer CSP'ler gibi CP ve CPS'ye uygun olarak faaliyet gösterirler.

7) TSA'ların ve bunlardan yararlanan abone ve güvenen diğer tarafların sorumluluk ve yükümlülükleri açıkça belirtilmiştir.

TSA anahtar üretimi ve yaşam döngüsü ve diğer ilgili tüm prosedürler ve güvenlik hususları en az EAL-4 seviyesinde olmalı ve CWA 14167-2 ve FIPS PUB 140-1'in şartlarını yerine getirmelidir.

8) TSA'da uygulanacak olan personel, fiziki ve çevre güvenliğine ilişkin hususlara yer verilmektedir.

9) TSA'nın faaliyetine son vermesi ve anahtarlarının çalınması ya da kopyalanması durumunda uygulanacak kurallar belirlenmiştir.

5 YAPILACAK DÜZENLEMELERDE BİLGİ GÜVENLİĞİNE İLİŞKİN OLARAK DİKKATE ALINMASI GEREKEN HUSUSLAR

Temel Prensipler

- Yapılan düzenlemeler, elektronik imza kullanımını yaygınlaştırmaya yönelik olmalıdır. Bu amaçla:

    - Elektronik imza kullanımı son kullanıcılar için kullanımı kolay olmalı
    - Alınan herhangi bir yöntemle kullanıma başlanan "imza oluşturma verisi" farklı ortamlarda (akıllı kart, bilgisayar, vb.) saklanabilmeli
    - Son kullanıcılar için elektronik imza kullanımı ucuz olmalı (ucuzluk sadece nitelikli elektronik sertifika alımı için ödenen bedel için değil, tüm donanım, yazılım, eğitim, hizmet ve diğer maliyetler göz önüne alınmalı)
- Kişisel bilgilerin gizliliği ve tutarlılığı garanti altına alınmalı. Bu amaçla:

    - "İmza oluşturma verisi"nin sahibi dışında herhangi bir kişi ve kuruluş tarafından kopyalanamaması, bilginin yedeğinin herhangi bir başka kurum ya da kuruluşa verilememesi sağlanmalı,
    - Kişiye özel şifreli bilgileri açmak için kullanılacak anahtarların, anahtar sahibi dışında bir başka kurum ve kuruluş tarafından talep edilememesi sağlanmalı,
    - Ancak, kişiler dilediklerinde, kaybolma ve arızalara karşı, bu anahtarları düzenli olarak denetlenen ve bu konuda atanmış kurum ya da kuruluşlara emanet edebilmeleri sağlanmalı. Emanet edilen anahtarların bu kurum ya da kuruluşlar tarafından kullanılamaması için gerekli ek güvenlik önlemleri üzerine çalışılmalı.

- Elektronik imza kullanımı son kullanıcılar için kullanımı kolay olmalı

    - Elektronik imza hazırlık süreci (elektronik sertifika alımı)
    - Elektronik imza oluşturma verisi'nin farklı saklama biçimleri desteklenmeli, sertifika hizmet sağlayıcıları ve elektronik imza kullanımını destekleyen tüm kurum ve kuruluşlar bu konuda hazırlanacak dokümanları ve diğer yardımcı materyalleri (broşür, el kitabı, web sitesi, yardım masası, vb.) tüm kullanıcılara ek bir maliyet almadan sağlamalı

- Hem bireyler, hem de kurumlar elektronik imza'nın getirdiği güvenlik özellikleri ve Internet vb. teknolojilerin kullanımından gelen ek güvenlik problemleri konusunda uyarılmalı

- Elektronik imza kullanacak kurumların bu kullanıma başlamadan önce almaları gereken güvenlik önlemleri belirlenmeli, bu konuda da belirli sertifikasyonlar ve akreditasyonlar önerilmeli

- Elektronik imzanın kullanımı konusunda farklı güvenlik seviyeleri kullanımına izin verilmeli. Bu güvenlik seviyeleri için hem akıllı kart, hem token ve benzerleri, hem de istendiğinde herhangi bir güvenlik donanımına ihtiyaç kalmadan kullanımı sağlanabilmeli.

- Onay kurumu ve müşteri arasındaki sorumlulukların açık şekilde tanımlanması ve hukuksal olarak da bu konuda bir düzenleme yapılması

- Herhangi bir sertifika sağlayıcıdan alınan sertifikanın diğer sertifika sağlayıcılar tarafından da kabul edilmesi veya çapraz sertifikasyon konusunda düzenleme yapılması

- Yaşanabilecek kötü niyetli kullanım veya adli olayların takibinin yapılabilmesi için Sertifika Hizmet sağlayıcının bulunduracağı kayıtların neler olduğunun belirlenmesi

- En alt seviyede sertifika belirlenirken hangi evraklar alınarak hangi seviyede sertifika verileceğinin belirlenmesi

- Sertifika otoriteleri ile Nüfus idaresi ve diğer resmi kurumlar arasında sertifika veriliş sürecinde nasıl bir ilişki olabileceğinin tanımlanması. Bu sayede sertifika verilmesi adımında istekte bulunan kişinin gerçek anlamda tanımlanması.

- Sertifika hizmet sağlayıcılarda çalışacak kişilerde bir güvenlik klerans seviyesinin istenmesi çalışanlar açısından güvenliğin sağlanması konusunda yararlı olacaktır.
- Hangi servisler ve işler için e-imza kullanılacağı tüm devlet kurumları tarafından ilişkide oldukları kurumlar da dikkate alınarak belirlenmelidir.

5.1 Türkiye'de elektronik imza ile ilgili standartlar konusundaki eksiklikler ve söz konusu eksikliklerin giderilmesi için yapılması gerekenler

Hizmet verecek sertifika hizmet sağlayıcıda aranması gereken temel standartlar konusunda eksiklikler mevcuttur. E-imza kanununda yetkilendirmenin herhangi bir lisanslama ile yapılacak şekilde düzenlenmemiş olması ve ayrıca bu hizmeti verecek kişilerde mecburi bir kriter aranmamış olması, özellikle güvenli ve belirli bir hizmet standardında hizmet veremeyecek kişi veya kurumların bu hizmeti vermeye çalışmasına neden olabilecektir. Bahsi geçen sebeplerden ötürü mutlaka iyi bir denetim mekanizmasının devrede olması gereklidir.

5.2 Yapılacak düzenlemelerde standartlara ilişkin olarak mutlaka yer alması veya atıfta bulunulması gerektiği düşünülen hükümler, söz konusu hükümlerin güncelliğinin korunması için öneriler

Sertifika hizmet sağlayıcının operasyonel olarak güvenli bir şekilde hizmet vereceğinin tam anlamı ile belirlenebilmesi için bazı temel standartların istenmesi uygun olacaktır. Bu standartlar arasında TS EN ISO 9001 gibi kalite standartlarının yanı sıra BS 17799 gibi bilginin güvenliğinin sağlanmasına yönelik standartlara uygunluk istenmelidir. Fakat tek başına bu hükümlerin yeterli olmayacağı da açıktır. Bu sebepten ötürü, ileride Telekomünikasyon Kurumu'nda veya diğer kuruluşlarda oluşturulacak tecrübe ve birikim ile Sertifika Hizmet sağlayıcılardan yukarıda belirtilen standartlara ek olarak farklı standartlar da istenebilmesine imkan tanıyan maddeler eklenmelidir. Burada önemli bir husus da sertifika hizmet sağlayıcıların akreditasyonudur. Akredite edilmiş sertifika hizmet sağlayıcılarının Telekomünikasyon Kurumu'nun denetimi etkin olarak yapmasını sağlayacağından, Türk Akreditasyon Kurumu (TÜRKAK) tarafından akreditasyon şartı aranmalı ve TÜRKAK, akredite edilmiş sertifika hizmet sağlayıcılarının listesini güncel olarak

kamuya duyurmalıdır. Belgelendirme ve akreditasyonda Avrupa Akreditasyon Birliği'nin (EA) yayınladığı EA-7/03 ve ISO/IEC Guide 62 dokümanları gözönüne alınmalıdır.

5.3 Sertifika hizmet sağlayıcılarında bilgi güvenliğine ilişkin olarak aranacak ilave şartlar

Bilgi güvenliği konusunda en temelde yönetim anlayışı ve operasyonel olarak güvenlik konusunda doğru çalışıldığını göstermesi açısından BS 7799 veya muadili Türk standardlarının (TS ISO/IEC 17799) aranmasında fayda vardır. Fakat bu standart temelde bilgi güvenliği risk yönetimi yapılıp yapılmadığını kontrol etmeye yönelik bir standarttır. Bu standarda ek olarak yönetmelikte yapılacak düzenlemeler ile sertifika hizmet sağlayıcıdan belirli alanlarda temel güvenlik standartlarını sağlaması istenmelidir. Bu alanlar aşağıdaki gibi sıralanabilir:

- **Fiziki Güvenlik ve Fiziki Erişim**

  - Verinin tutulduğu ortamlara, mekanın en dışından başlanararak içeriye doğru güvenlik koridorları oluşturulmalıdır. Bu güvenlik koridorları, fiziki erişim ve elektronik cihazlarla erişim başlıkları ile iki ana konuda ele alınmalı ve her biri için ayrı ayrı güvenlik politikası uygulanmalıdır. Güvenlik koridorlarının denetlenmesi ve güvenlik politikalarının uygulanması esnasında ortaya çıkabilecek aksaklıkların önceden tespiti amacıyla simulasyon ortamlar oluşturulmalıdır.

  - Verinin tutulduğu/işlendiği ortamlara fiziki erişim düzeylendirilmeli, yetkiler paylaşımlı hale getirilmelidir.

  - Erişim yetkileri yazılı hale getirilip, görevli personelin erişebileceği güvenli ortamlarda tutulmalı, muhtemel aksaklıklar gözönünde tutularak her an yedek görevli personel bulundurulmalıdır. Üçüncü taraf destek hizmetleri gerektiği durumlarda, bu destek hizmeti görevli personel nezaretinde alınmalı, erişim yetkileri sınırlı tutulmalı, üçüncü taraflarlara herhangi bir kaydedici cihaz (ses, görüntü vs) ile güvenlik ortamlarına giriş izni verilmemelidir.

- Doğal felaketlere karşı tedbirler alınmalı, ana merkez bilgi işlem cihazları ile online senkranizasyon olan aynı (veya daha yüksek kapasiteli) konfigurasyona sahip cihazlar, farklı deprem veya doğal felaket kuşağında bulunan bölgelerde muhafaza edilmelidir. Her şartta Erişebilirlilik garanti altına alınmalıdır.

- **Sistemlerin uyumluluğu ve cihazların güvenliği**

  - Sistem bileşenlerinin tamamının uyumlu olduğu garanti edilmelidir.

  - Kullanılan cihazların elektromanyetik radyasyonunun önlenmesi için gerekli filtrelemeler yapılmalı, bu hususta TSE'nin yayınladığı Türk Standartları gözönünde bulundurulmalıdır.

  - Sistemlerin çalışmasını sürekli hale getirmek ve elektriğin açabileceği sorunlara karşı tedbir almak amacıyla güç kaynakları ve jeneratörler kullanılmalıdır.

  - Cihazların periyodik bakımları imalatçı/satıcı önerisi doğrultusunda yapılmalıdır.

  - Yazılımlar ve diğer ara birimler virüs ve benzeri ataklara karşı korumalı olmalı, görevli personel böyle durumlarda mail, telefon vs araçlarla otomatik olarak uyarılmalıdır.

  - Tüm anahtarlar güvenli ortamlarda saklanmalı, gerektiğinde kriptolama teknikleri veri saklama işlemlerinde de kullanılmalıdır.

  - Sisteme her türlü erişim yazılımlar aracılı ile takip edilmeli, log'lar tutulmalıdır.

- **Çalışanlarda aranması gereken özellikler**

  - Güvenlik konusunda eğitimli personel çalıştırılmalı, gelişen teknolojiler hakkında personelin yetişmesi için gerekli eğitimler ilgili personele verilmelidir.

  - Üçüncü tarafların (yazılım ve donanım destek hizmeti, temizlik hizmeti, kısa süreli çalıştırılan personel, danışmanlık hizmetleri vs) fiziki ve elektronik erişimleri, hizmetlerin aksamaması ve güvenliği tehlikeye atmayacak şekilde denetlenmeli, işlemler dokümante edilmelidir. Üçüncü taraflarca yapılacak her işlem sözleşme hükümlerine bağlanmalıdır.

  - Yanlış kullanımdan doğacak sonuçlarla, diğer personel hatalarının doğuracağı risklere karşı her türlü idari ve teknik tedbirler alınmalıdır.

  - Personelin yetkileri hiyerarşik ve otokontrol sağlayıcı biçimde yapılandırılmalıdır.

  - Personelin işe alımlarında, ilgili yasalarda belirtilen yasal şartları taşıma şartı aranmalı, teknik yeterlilikleri (mezuniyet bilgileri, aldıkları eğitimler vs) belgelendirilmelidir.

  - Personel ile hizmet sağlayıcı kuruluş arasında imzalanacak iş akitlerinde gizlilik ve mahremiyet kuralları öncelikli madde olarak bulunmalıdır.

  - İşe alma veya sözleşme şartlarında bir değişiklik oluştuğunda, özellikle personelin işletmeden ayrılma aşamasında olduğunda veya sözleşme süresi sona erme aşamasında olduğunda, gizlilik anlaşmaları ve güvenlik politikaları yeniden gözden geçirilmelidir.

- **Sertifika Hizmet Sağlayıcılığı ve Hizmetinin Sürekliliği**

    - Sertifika Hizmet Sağlayıcılığı yetkisi, akreditasyon kuruluşları ile akredite edilmelidir.

    - Akreditasyon işlemini, yerli akredidasyon kurumları yapmalı, teknik yetersizlik dolayısıyla yapılması mümkün olmazsa, yerli akreditasyon kurumlarından yetki alan yabancı akreditasyon kurumlarına yaptırılmalıdır. Bu konuda uluslararası anlaşmalar öncelikli dir.

    - Doğal afetler ve diğer felaketler karşısında hizmetlerin sürekliliğinin nasıl sağlanacağı ayrıntılı bir biçimde dökümante edilerek ayrıntılı bir biçimde planlanmalı, bu planın bir kopyası otorite kuruma sunulmalıdır.

5.4 Kullanıcıların bilgi güvenliği ile ilgili olarak dikkat etmesi gereken hususlar

- Kullanıcıya yönelik olarak kitapçıkların hazırlanması ve bu konudaki standartların belirlenmesi.

- Anahtar yönetimindeki temel konuların belirlenmesi

    - Anahtarların kaybedilmesi durumunda nasıl yenileneceği

    - Anahtar sahibinin ortadan kalması durumunda nasıl bir süreç ile anahtarların yetkinliğinin ortadan kaldırılması

5.5 Güvenli elektronik imza oluşturma araçlarının uygunluk denetiminin yapılmasında kullanılabilecek yöntemler ve Türkiye'de söz konusu denetimin yaptırılabileceği özel/kamu kuruluşları

- Denetim konusunda bilgi güvenliğine yönelik olarak tecrübe sahibi belgelendirme kuruluşları ve mevcut ise Türk Akreditasyon Kurumu tarafından akredite edilmiş denetim/belgelendirme kurum ve kuruluşları tercih

edilmelidir (Bu konuda yabancı firmaların Türkiye'deki temsilciliklerinde de TÜRKAK'tan akredite olma veya yabancı akreditasyon kurumu ile TÜRKAK arasında akreditasyonun tanınması konusunda ikili anlaşma şartı aranmalıdır).

- Sadece bilgi güvenliğine yönelik denetimler yeterli olmayacaktır, bu denetimlere ilave olarak ve hatta daha da öncelikli olarak operasyonel anlamda denetim de yapılması gereklidir. Bu denetimin yapılmasında sertifika otoritesinin hazırlayacağı "Sertifika Uygulama Dökümanı" ve "Sertifika Politikası Döküman"larına ne derecede uyulacağı denetlenmelidir.

- İleride yapılacak denetimlerin referans alınabileceği bir standart hazırlanıp kullanılabilmesi sağlaması açısından hazırlanacak yönetmelikte Telekomünikasyon Kurumu'nun ileride Sertifika Otoritelerinden başka kriterler de isteyebileceği belirtilmelidir.

5.6 Güvenli elektronik imza doğrulama araçlarının geliştirilmesini ve son kullanıcılar tarafından kullanımını teşvik etmek için öneriler

1. Sertifika yönetim işlemlerinin kolay olmasının sağlanması (dağıtım, iptal, yenileme, vb)
2. Sertifika sahiplerinin sistemin işleyişi hakkında sağlıklı bilgilendirilmesi

Uyumluluk ve standartların netliğiyle ilgili olarak

1. Uygulamada ve standartlarda kullanıcı işlemlerinin uzatılmaması
2. Kullanılacak cihazlara ilişkin (token veya kart gibi) alternatiflerin artırılması ve kolay erişilebilir olması
3. Zaman damgası konusunda bilgilendirme yapılması ve işlemlerin kolay olmasına dikkat edilmesi

Maliyetlerle ilgili olarak

1. Cihaz maliyetlerinin (token, kart, vb) makul düzeyde tutulması
2. İşletim ve sertifika fiyatlarının makul tutulması

6 SONUÇ VE ÖNERİLER

Sonuç olarak elektronik imza uygulamalarında Avrupa Birliği tarafından halen kullanılmakta olan ve bu raporda belirtilen direktif ve standardların Türkiye'de de uygulanması için gerekli idari ve teknik altyapı hazırlıklarının süratle yapılması, akreditasyon ve belgelendirme süreçlerinin hassasiyetle kontrol altında tutulması ve izlenmesi sistemin verimli çalışması ve yaygınlaşması açılarından önem arzetmektedir.

7 YARARLANILAN KAYNAKLAR

1. 12 Nisan 2000 tarihli İsviçre Sertifika Hizmetleri Tüzüğü
2. Avrupa Standardlar Teşkilatları bibliyografik standard veritabanları
3. RegTP (Regulierungsbehörde für Telekommunikation und Post), Digital Signatures
4. TS ISO/IEC 17799 standardı
5. EA-7 EA Guidelines for tha accreditation of bodies/operating certification/ registration of Information Security Management Systems, Feb. 2000
6. www.european-accreditation.org
7. www.europa.eu.int