ELEKTRONİK İMZA
ULUSAL KOORDİNASYON KURULU
HUKUK ÇALIŞMA GRUBU
İLERLEME VE SONUÇ RAPORU

Temmuz, 2004
İstanbul

İÇİNDEKİLER

KISALTMALAR CETVELİ

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

BİRİNCİ KISIM – "SUNUŞ"

Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu olarak bu zamana kadar yapılmış olan çalışmaları derlediğimiz bu raporun, Telekomünikasyon Kurumu nezdinde "5070 Sayılı Elektronik İmza Kanunu" ile ilgili çıkarılacak olan yönetmeliklerin hazırlanması sırasında Kurum ve kamuoyuna yol gösterici olacağına inanmaktayız.

Çalışmamızda, sonuç ve ilerleme raporunu bir arada Kurum nezdinde kamuoyunun ilgilerini sunmayı uygun gördük. Hukuk Çalışma Grubu kanunun sistematiğine ve hukukun temel ilkelerine bağlı kalarak, Elektronik İmza Ulusal Koordinasyon Kurulu'nun Alt Yapı, Bilgi Güvenliği ve Standartlar çalışma gruplarının ortaya koydukları değerli çalışmaları, Avrupa Birliği ve üye ülkelerin kanunlaştırmaları ve düzenlemelerini, uluslar arası alandaki düzenleyici otoritelerin yayınladıkları politika metinlerini telif edici bir çerçevede, hukuk çalışma grubunun bütünleştirme misyonuna uygun bir biçimde ortaya koymaya çalışmıştır.

Yapılan bu çalışmanın şüphesiz en can alıcı noktasını 13 Nisan 2004 tarihinde Telekomünikasyon Kurumu'nda yapılan Ulusal Koordinasyon Kurulu toplantısını müteakiben tertip edilen toplantılar ve bu toplantılarda katılımcılarla yapılan fikir alışverişleri ve tartışmalardan elde edilen verilerin harmanlandığı YÖNETMELİK ŞABLONU TASLAĞI oluşturmaktadır. Bu Taslak metnin oldukça kısa bir süre zarfında olgunlaştırılmasını ise, Telekomünikasyon Kurumu'nun bizlere sağladığı kollektif çalışma ortamına borçlu olduğumuzu özellikle belirtmek ve Kuruma gerek şahsım gerek Hukuk Çalışma Gurubu adına teşekkür etmek isterim. Yönetmeliğe nihai görüntüsünü verecek olan Kurumda görevli olan arkadaşlarla, Hukuk Çalışma Gurubu üyelerinin ortak toplantılarında yaratılan sinerji, bu başarıda önemli bir role sahiptir.

Hazırlanan Yönetmelik Şablonu Taslağında, uluslararası metinler hazırlanırken göz önünde bulundurulan şu iki ilke özellikle dikkate alınmıştır:

1. Son kullanıcı (Tüketici) bakımından sistemin kolay işlemesi
2. Yine son kullanıcı bakımından sistemin maliyetinin düşük, ucuz olması ve bu sayede elektronik imza kullanımının yaygınlaştırılması.

Telekomünikasyon Kurumu'nun da bundan sonra elektronik imza ile ilgili yapacağı diğer düzenlemelerde dikkate alması gereken ilkeler bunlardır. Bunun yanı sıra Kurumun diğer bir vazifesi de; bu alanda piyasada rekabeti teşvik edecek, sektörün gelişmesini, genişlemesini sağlayacak regülasyonlar yapılmasına özen göstermektir. Özellikle Elektronik İmza Kanunu md. 21'deki *"denetim"*'e ilişkin hüküm, lafzı itibariyle kamu ve özel sektör arasında daha işin en başından haksız rekabete neden olacak bir niteliğinde olduğu için, Kurum'un bu hükmün sakıncalarını asgariye indirecek bir davranış sergilemesi beklenmektedir. Yine Sertifika Hizmet Sağlayıcıların faaliyetlerine ilişkin olarak Kurum tarafından belirlenecek ücret politikasının da sektör ve son kullanıcılar dikkate alınarak, piyasanın önünü açacak ve elektronik imza kullanımını yaygınlaştıracak yapıda olması gerekecektir.

Alt Yapı Çalışma Gurubu Raporunda yer alan ve kamu tüzel kişilikleri nezdinde yapılan Anket sonuçları içinde özellikle dikkati çeken nokta, tüm bu kurumların e-imza konusunda eğitime ve bilgiye ihtiyaçları olduğunu ifade etmeleridir. Gerçekten henüz çok yeni olan elektronik imza kurumunun gerek kamu-özel sektöre ve gerekse bireylere anlatılması ve toplumun bu konuda bilinçlendirilmesi önem taşımaktadır. Elektronik Ticaretin ivme kazanması ve bu doğrultuda şirket ve bireylerin bu pastadan daha çok pay almalarının sağlanması isteniyorsa, Telekomünikasyon Kurumu'nun bir an önce bu gurupları elektronik imzanın yararları, getireceği kazançlar, kolaylıklar konusunda bilgilendirmeye başlaması gerekmektedir. Kurumun omzuna yüklenen bu vazife ve diğer vazifelerde de, kendilerine İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi olarak her zaman destek olabileceğimizin altını çizmek isterim.

Çalışmamız altı temel kısımdan oluşmaktadır. İlk kısım "Sunuş", ikinci kısım "Yazarlar", üçüncü kısım "Yönetici Özeti", dördüncü kısım "Elektronik İmza Ulusal Koordinasyon Kurulu Bilgi Güvenliği ve Standartlar Çalışma Grubu ile Alt Yapı Çalışma Grubu Raporlarının Değerlendirilmesi", beşinci kısım "Hukuk Çalışma Grubu İlerleme Raporu", altıncı ve son kısım ise "Sonuç Raporu" başlıklarından oluşmaktadır. "Sonuç Raporu" kısmı dört temel bölümden oluşmaktadır. İlk bölüm, 5070 Sayılı Elektronik İmza

Kanunun genel bir değerlendirmesini yapmaya yöneliktir. Altıncı kısmın ikinci bölümü Elektronik İmza Kanunun 20. maddesi uyarınca düzenlenecek yönetmeliklerle ilgili atıfta bulunulan maddelerin açıklanması ve yönetmelikler çıkartılırken dikkate alınması gereken temel prensipleri açıklamaya çalışmaktadır. Üçüncü bölüm ikinci bölümde yapılan açıklamalar doğrultusunda ortaya konulan "Yönetmelik Şablonu Taslağı"nın açıklanmasına yöneliktir. Dördünce ve son bölüm ise "Sonuç ve Öneriler" başlığını taşımaktadır.

Hukuk Çalışma Gurubu Başkanlığı görevimin yanısıra, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Direktörü olarak benim, gerek Merkez Danışma Kurulu Üyesi olan ve gerek Hukuk Çalışma Gurubu Başkan Yardımcısı ve Raportörü olarak bana destek veren değerli arkadaşlarım Sayın Yasin BECENİ, Tuğrul SEVİM ve Adalet Bakanlığı Bilgi İşlem Dairesi Tetkik Hakimi Mesut ORTA'ya, Murat LOSTAR ve Mete VARAS'a bu çalışmanın başından beri gösterdikleri yardımseverlik, özveri, disiplin ve çalışma azminden dolayı teşekkür ediyorum. Diğer iki Çalışma Gurubunda görevli arkadaşlara da, hazırladıkları raporlarla son derece teknik konulara ilişkin olarak yapacağımız düzenlemelerde bizlere ışık tuttukları, yardımcı oldukları için teşekkür ediyorum.

Çalışmamızın Elektronik İmza ile ilgili yapılacak düzenlemelerde yararlı olmasını diler, çalışma grubum adına hukuk çalışma grubu raporunu Telekomünikasyon Kurumunun ve Kurum nezninde tüm kamuoyunun ilgi ve değerlendirmelerine sunarım.

Yrd. Doç. Dr. Leyla KESER

Elektronik İmza Ulusal Koordinasyon Kurulu

Hukuk Çalışma Grubu Başkanı

İKİNCİ KISIM – "YAZARLAR"

Yrd. Doç. Dr. Leyla KESER – İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Müdürü

Yasin BECENİ - Türkekul Hukuk Bürosu/ İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Danışma Kurulu Üyesi

Tuğrul SEVİM - Türkekul Hukuk Bürosu / İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Danışma Kurulu Üyesi

KATKIDA BULUNANLAR

Murat LOSTAR – Lostar Bilgi Güvenliği A.Ş. Yönetim Kurulu Başkanı

Mete VARAS - TurSign Genel Müdürü

Can ORHUN - Siemens Business Services Sistem Hizmetleri A.Ş. Ürün Müdürü

ÜÇÜNCÜ KISIM – "YÖNETİCİ ÖZETİ"

5070 Sayılı Kanun hazırlanırken yabancı mevzuattaki benzer düzenlemeler ve Avrupa Komisyonu'nun 99/93/EC sayılı elektronik imzalara ilişkin Direktif'i temel alınmıştır. Ancak Kanun metni oluşturulurken örnek alınan metinlere sadık kalınmaması ve bazı önemli konuların düzenlenmemesi uygulamada problemlere yol açabilecektir. Bu problemlerin ortaya çıkması Yönetmelikle yapılacak düzenlemelerle önlenebilir.

Raporun temel metni altıncı kısım içerisinde bulunmaktadır. Altıncı kısım dört temel bölümden oluşmakta bu bölümler hazırlanırken, öncelikle Kanunun çizdiği hukuki çerçeveye bağlı kalınmaktadır. Bu nedenle bu kısmın ilk bölümü Kanunun değerlendirilmesine ayrılmış ve Kanunun hükümleri karşısında uygulamada ortaya çıkabilecek problemler tespit edilmiştir. İkinci bölümde Yönetmelikle düzenlenecek kanun hükümleri ile ilgili öneriler, Yönetmelik Şablonu Taslağı temel alınarak açıklık getirilmiştir. Yönetmelik Şablonu Taslağı'nın temel amaçları; ülkede güvenli bir elektronik imza alt yapısı oluşturmak, elektronik sertifika ve elektronik imza kullanımını yaygınlaştırmak, Kanunun düzenlediği bazı hususları Yönetmelikle açıklamak suretiyle Kanunun yanlış yorumlanmasından doğabilecek sorunların önüne geçmek olarak özetlenebilir. Üçüncü bölüm ise ikinci bölümde açıklanan şablonun somutlaştırılmasına yöneliktir.

Yönetmelik şablonu taslağı, güvenli elektronik imza oluşturma araçlarında lisans zorunluluğu, sertifika hizmet sağlayıcının sağlaması gereken hukuki ve teknik asgari kriterler, sertifika kayıt ve dağıtım yolları, uyulması gereken uluslararası standartlar ve yabancı sertifikaların garanti edilmesinde kullanılması gereken yöntemler gibi konulara açıklık getirilmeye çalışılmıştır. Ayrıca açık anahtarlı alt yapı hizmetlerinin sağlanmasında, bir çok bileşenin bulunması sebebiyle bu bileşenlerden hangisinin *"elektronik sertifika hizmet sağlayıcının"* yükümlülüklerine tabi olacağı hususuna da açıklık getirilerek elektronik sertifika hizmet sağlayıcısı kavramının hukuki kapsamı somut bir şekilde açıklığa kavuşturulmuştur.

Raporun Sonuç bölümünde ise, şimdiye kadar fotoğrafını çektiğimiz bu durumdan çıkardığımız, geleceğe yönelik olarak atılması gereken adımların, izlenmesi gereken politikanın neler olabileceği şeklindeki değerlendirmelerimize yer verilmiştir

DÖRDÜNCÜ KISIM – "ELEKTRONİK İMZA ULUSAL KOORDİNASYON KURULU BİLGİ GÜVENLİĞİ VE STANDARTLAR ÇALIŞMA GRUBU İLE ALT YAPI ÇALIŞMA GRUBU RAPORLARININ DEĞERLENDİRİLMESİ"

1. Alt Yapı Çalışma Grubu İlerleme Raporunun Değerlendirilmesi

Elektronik İmza Ulusal Koordinasyon Kurulu Alt Yapı Çalışma Grubu'nun hazırlamış olduğu raporda yurtdışı örnek uygulamalar ve ülke içindeki mevcut durum ve talepler açıklıkla ortaya konulmuştur. Rapordan anlaşıldığı üzere kamu kurumlarının çoğunun kısa vadede elektronik imza uygulamaları ve çözümleri ortaya koyma planları bulunmaktadır. Ancak bu kurumların konuyla ilgili en büyük problemi bilgi eksikliğidir. Bu eksikliğin giderilmesi için kamu kurumlarına elektronik imzanın hukuki ve teknik yönleriyle ilgili bilgilendirme çalışmaları yapılmalı ve bu kurumlara elektronik imza kullanımıyla ilgili uygulama projeleri geliştirilmelidir.

Alt Yapı Çalışma Grubu'nun raporunda dikkat edilmesi gereken bazı hususlar bulunmaktadır. Raporda elektronik imzanın fonksiyonları olarak,

1. Sistem girişleri (loginler) ve erişimler
2. Bilgisayar ortamında belge ve verileri elektronik olarak imzalamak
3. Bilgisayar ortamında belge ve verileri elektronik olarak şifrelemek

gösterilmiştir. Ancak kanunda yapılan açık tanım dolayısıyla elektronik imza sadece "imzalama" işlevidir. Sistem girişi veya şifreleme işlemleri, elektronik imza değildir ve bu işlemler Kanun kapsamında değerlendirilemez. Açık anahtarlı altyapı kullanılarak yapılan sistem girişi ve şifreleme işlemleri de Kanun kapsamına girmemektedir. Sadece sistem girişi ve şifreleme amacıyla yayınlanan sertifikalar ve bu sertifikaları yayınlayan kurumlar da Elektronik İmza Kanunu kapsamına girmemekte ve Kanunda belirtilen gereksinimlere ve yükümlülüklere tabi olmamaktadırlar. Ayrıca Kanunda yapılan güvenli elektronik imza tanımı sebebiyle, güvenli elektronik imzaların sadece açık anahtarlı altyapı kullanılan bir sistemde oluşturulabilmelerine rağmen; Kanun bütün elektronik imzaları kapsamına almakta ve bütün elektronik imzalara hukuki bir değer tanımlamaktadır. Ancak burada dikkat edilmesi gereken husus, elle atılmış imza ile eşit hukuki değere sahip tek elektronik imza güvenli elektronik

imzadır ve o da açık anahtarlı altyapı kullanılarak oluşturulabilir. Sonuç olarak 5070 sayılı Elektronik İmza Kanunu kapsamındaki elektronik imza kavramı, açık anahtarlı altyapı teknolojisiyle sınırlanamaz.

Ayrıca güvenli elektronik imza kullanımıyla ilgili en önemli sorunlardan biri olan farklı açık anahtarlı altyapı alt alanlarının birbirini tanıması ve karşılıklı işlerlilik sorunuyla ilgili bir incelemenin Alt Yapı Çalışma Grubunun raporunda incelenmesi gerekir. Sertifika hizmet sağlayıcıların kendi aralarında çapraz sertifikasyon veya çapraz tanıma sistemlerinden hangisini uygulamasının daha verimli sonuçlar ortaya konacağı yapılacak çalışmayla açıklığa kavuşturulmalıdır. Hukuki açıdan konuyla ilgili görüşümüz; çapraz sertifikasyonun sertifika hizmet sağlayıcıları arasında hem teknik hem de hukuki uyumluluk gerektirmesi ve bu uyumluluğun piyasaya girecek her yeni oyuncu için tekrar sağlanmak zorunda olması, bu sistemin kullanılabilirliğinin düşük olduğu yönündedir. Çapraz sertifikasyon yapılabilmesi için en azından hukuki açıdan, her iki sertifika hizmet sağlayıcısının sertifika politika belgelerinin (CP) ve sertifika uygulama hükümlerinin (CPS) birbirlerine uyumlu olması gerekmektedir. Yaklaşık yüz sayfa civarında olan ve yükümlülükler ve teknik hususlar konusunda oldukça ayrıntılı bilgiler içeren bu belgelerin uyumlaştırılması, sertifika hizmet sağlayıcılar ağır maddi yük getirecektir. Bu sebepten ötürü uyum gerektirmeyen çapraz tanıma (cross-recognition) sisteminin de sertifika hizmet sağlayıcılar tarafından kullanılabilmesi gerekir. Kanaatimizce bu sorunla ilgili olarak ortaya konacak en doğru çözüm, sertifika hizmet sağlayıcıları sistemlerden birini seçmeye mecbur etmemektir. Yönetmelikte konuyla ilgili, sistem seçme zorunluluğuna yönelik bir düzenleme yapılmamalıdır.

2. Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporunun Değerlendirilmesi

Elektronik İmza Koordinasyon Kurulu Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu'nda, elektronik imzayla ilgili uluslarası standartlar incelenmiş ve konuyla ilgili temel ilkeler ortaya konulmuştur. Hukuk Çalışma Grubu Raporu'nun hazırlanmasında, Bilgi Güvenliği ve Standartlar Çalışma Grubu'nun Raporunda incelenen standartlardan faydalanılmış, Yönetmelik Şablonunda bu standartlara yer verilmiştir.

Bilgi Güvenliği ve Standartlar Çalışma Grubu'nun Raporunda dikkat edilmesi gereken bir husus, Rapor'da sadece donanım bazlı araçların, güvenli elektronik imza oluşturma aracının niteliklerine sahip olabileceğinin belirtilmiş olmasıdır. Ancak Kanunun güvenli elektronik imza oluşturma araçlarıyla ilgili hükmünde açıkça bu araçların yazılım veya donanım bazlı olabileceği belirtilmiştir. Ayrıca piyasada da yazılım bazlı güvenli elektronik imza oluşturma araçları bulunmaktadır.

Bilgi Güvenliği ve Standartlar Gurubunun hazırladığı Raporda, sertifika hizmet sağlayıcıların akreditasyonuna ilişkin bazı ifadeler yer almaktadır. 5070 sayılı Kanun sertifika hizmet sağlayıcıların akreditasyonu konusunda hiçbir hüküm içermediği için, kendilerini akredite ettirip ettirmemek sertifika hizmet sağlayıcıların takdirindedir. Bu konuda kanunda açıklık olmadığı için, yönetmelikle, kanunda düzenlenmeyen bir konuda düzenleme öngörülmesi hukuken imkansızdır.

BEŞİNCİ KISIM – "HUKUK ÇALIŞMA GRUBU İLERLEME RAPORU"

YAPILAN ÇALIŞMALAR

a. Birinci Toplantı

Eski Başkan Doç. Dr. Haluk KONURALP ile 13 Nisan 2004 tarihinde Telekomünikasyon Kurumu'nda yapılan Ulusal Koordinasyon Kurulu toplantısını müteakip, 29 Nisan 2004 tarihinde yine Telekomünikasyon Kurumu'nda geniş katılımlı Hukuk Çalışma Gurubu toplantısı yapılmıştır. Bu toplantıda Yönetmeliğe ilişkin olarak üzerinde durulan konular aşağıdaki gibidir:

- Öncelikle Yönetmeliğin adının ne olması gerektiği (Kanunla aynı adı mı taşısın, farklı bir ad mı verelim?) tartışıldı
- Birden çok Yönetmelik düzenlenmesinin gerekli olup olmadığı konuşuldu,
- Tek tek Yönetmelikte düzenlenecek maddeler ve Yönetmelikte bulunması gereken konular hakkında karşılıklı görüş alışverişinde bulunulmuştur,
- Sayı itibariyle oldukça kalabalık olan bu gurup içinden daha küçük bir Alt Çalışma Gurubu tespit edilmiştir. Alt Çalışma Gurubu aşağıdaki isimlerden oluşmaktadır:

1. Birsen ACIR
2. Feyzan TORLAK
3. Leyla DAYANIR
4. Aslıhan ÖZDEMİR
5. Seran ERATAY
6. Mesut ORTA
7. Metin Hakan ATİLA
8. Yasin BECENİ
9. Sedat GÜRGEN
10. Tuğrul SEVİM
11. Ümit IŞIK
12. Mete ÇANGA
13. Çiğdem ÇAMURDAN

Söz konusu toplantıda Yönetmelikte açığa kavuşturulması gereken konulara ilişkin olarak, oluşturulan Alt Çalışma Gurubu üyeleri arasında aşağıdaki şekilde bir görev dağılımı yapılmıştır:

1. Sertifika Hizmet sağlayıcıların çalıştıracakları personelin nitelikleri (Mete ÇANGA-DPT)
2. İmza oluşturma verisi oluşturma prosedürü, kurum politikası, risk analizi (Tuğrul SEVİM-Türkekul Hukuk Bürosu)
3. Sertifikanın zorunlu ve ihtiyari içeriği (Birsen ACIR-SPK)
4. Saklama/Doğrulama/Şifre değişikliği (Mesut ORTA-Tetkik Hakimi Adalet Bakanlığı)

Dağıtılan görev paylaşımıyla ilgili raporların teslim tarihi olarak 10 Mayıs Pazartesi günü kararlaştırılmıştır.

b. İkinci Toplantı

Hukuk Çalışma Gurubu olarak ikinci toplantı, yine Telekomünikasyon Kurumunda, 26.5.2004 tarihinde daha sınırlı katılımcı gurubu ile gerçekleştirilmiştir. Toplantıda şu konular üzerinde tartışılmıştır:

Mesut ORTA; tarafından, kamu kurumlarında e-imzaya yönelik genel eğilimlerin tespitine ilişkin bir anket yapıldığı belirtilmiştir. Sertifika kurumları kendi sertifikalarını başka kurumlarla nasıl paylaşacak? Kamu kurumları açısından bu paylaşımın Telekomünikasyon Kurumu üzerinden yapılıp yapılmayacağının tartışılmasını istemiştir. Yine zaman damgası konusunun yönetmelikte nasıl düzenlenebileceği hususunun üzerinde durulması gerektiğinin altını çizmiştir.

Çiğdem ÇAMURDAN ise; sertifika hizmet sağlayıcı faaliyetine son vermesi durumunda hizmetin devamı nasıl sağlanacak? Bu durumdaki bir sertifika hizmet sağlayıcının verdiği

sertifikaların durumu ne olacak? Mevcut Yasada sertifika hizmet sağlayıcıların sorumlulukları ağır? Kanun yürürlüğe girdikten sonra özellikle kamu kurumları sertifika kurumu olmak için müracaat ettiğinde durum ne olacak? Şeklindeki sorunların tartışılmasını istedi.

Leyla KESER: Zorunlu Mali Mesuliyet Sigortası açısından durum nedir? Sertifikaları hangi formda vereceğiz? Yazılım? Donanım?

Feyzan TORLAK: Müşterilerin elindeki sertifikaların hangilerinin tanınacağı sorunu? Hangi işlemlerde güvenli elektronik imza kullanılacak?

Haluk KONURALP: Kullanıcının sorumluluğu konusu sertifika hizmet sağlayıcının bilgilendirme yükümlülüğü kapsamında değerlendirilebilecektir. Sertifika sahiplerinin sorumluluğu nasıl bir sorumluluktur?

Yasin BECENİ: Kanunda tanımlanan Yönetmelik kapsamına neler girecek iyi belirlenmeli? Kamu-kamu, kamu-özel kurumlar arasındaki çapraz sertifikasyon sorunu? Birçok noktada Telekomünikasyon Kurumuna ileride tebliğlerle sorunu çözebilmesini sağlayacak yol gösterilmelidir. Uygulama açısından kök sertifika, alt sertifika otoritesi gibi kavramlara takılmak gereksiz. Bu işin doğası gereği mevcut olacakları için bu kavramların ayrıca tanımlanmasına gerek yoktur. Ancak eğer istisna edilen bir model kullanılacaksa, dünya standartlarından ayrı olarak, sadece bunun tanımlanması gerekir. E-imza kurumlar bünyesinde daha çok uygulama alanı bulacaktır.

RAPORLARIN DEĞERLENDİRİLMESİ

Sn. TARIK METE ÇANGA'NIN RAPORU

Sertifika kurumlarında çalışacak personelin nitelikleri Kanun md. 10. md. 10'da hizmetin gerektirdiği nitelikte personel diyor. Bunu iki açıdan düşünmeli ve hem olumlu özellikler hem de olumsuz özellikler belirlenmeli.

Olumsuz Özellikler: Sertifika hizmet sağlayıcısının 10. madde gereği istihdam ettiği personelin taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya üç ay hapis yahut basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istismal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı veya vergi kaçakçılığına teşebbüs ya da iştirak veya bilişim alanındaki suçlardan dolayı hüküm giymemiş bulunması gerekir.

Olumlu özellikler: Kriptografi, bilgi güvenliği (PKI bilgisi, ağ güvenliği), bilgisayar mühendisliği, veri tabanı mühendisliği, alanlarında yeteri kadar uzman bulundurmak (bu sayının ne kadar olacağı tekrar düşünülecek. (Bu tür da ağ yönetimi.....alanlarında.....sahip olması gerekir). Ve bu personelin yeterli mesleki deneyime sahip olması gözetilir. Sertifika hizmet sağlayıcısı bu personeli hangi organizasyon şeması çerçevesinde çalıştıracağını tespit etmek zorundadır.

Sn. TUĞRUL SEVİM'İN RAPORUNUN DEĞERLENDİRMESİ

Elektronik İmza Kanunu'nun 10. maddesinin d bendinde imza oluşturma verisinin yaratılmasıyla ilgili prosedürün gizliliği ve güvenliği ile ilgili genel yükümlülükler ortaya konmuştur. Buna göre imza oluşturma verisi, yaratılma yeri bakımından, iki şekilde yaratılabilir;

a. Sertifika hizmet sağlayıcı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde
b. Sertifika hizmet sağlayıcının sağladığı araçlarla sertifika hizmet sağlayıcıya ait olmayan yerlerde

Burada sayılan yöntemler dışında imza oluşturma verisi sağlayıcı tarafından temin edilmemiş sertifika sahibine at araçlarla da üretilebilir.

Burada tartışılması gereken bir diğer konu imza oluşturma verisinin üretilmesi sürecinde bulunacak kişilerin kimler olacağıdır. Son kullanıcı sertifikaları için üretilen ima oluşturma ve doğrulama verilerinde (açık ve kapalı anahtar), veri ister sertifika talep eden kişi tarafından üretilsin ister sertifika sağlayıcı tarafından üretilin, üretme süresi otomatik olarak gerçekleşmektedir. Bu süreç sırasında yetkili kişilerin imza oluşturma verisi üretimine katkıda bulunmaları veya tanıklık etmeleri mümkün değildir.

Uygulamada yetkili kişilerin kapalı anahtar (imza oluşturma verisi) üretimine katıldıkları süreç "sertifika sağlayıcıların" kapalı anahtarlarının oluşturulması sürecidir. Buna göre eğer bir sertifika sağlayıcı, başka bir sertifika sağlayıcıya sertifika sağladığında, başka bir tanımla onu al sağlayıcısı (sub CA) yaptığında bu süreçte etili kişilerin bulunması gerekmektedir.

Sn. BİRSEN ACIR'IN RAPORUNUN DEĞERLENDİRMESİ

Sn. ACIR, Utah Eyaleti Dijital İmza Kanunu'nun bir kısım bölümlerini Türkçe'ye çevirerek çalışma grubunun ilgisine sundu. Çalışma Grubu Sn. Acır'ın sunduğu belge üzerinde aşağıdaki hususları tartışmaya açmıştır.

Utah MD. 1/L

İmza kanunu md. 9/ı bendindeki "maddi sınırlamalar" kavramının ne zaman hukuki bir uyarı olarak anlaşılması gerektiği , ne zaman özel bir yazılımla birlikte işlem yapma engeli halinde olacağı da yönetmelikte ayrı ayrı düzenlenmelidir.

Utah md. 1/M

Türk İmza kanunu md. 11 sertifika hizmeti askıya alındığında ne olacak??? Sertifika askıya alındığında ne olacak???

Sertifika hizmet sağlayıcının faaliyeti askıya alındığında (durdurulduğunda) kurum, directory services ve sertifika iptal listelerini devralır (sertifikalara ilişkin bilgilerin kurum tarafından

mı yoksa kurum tarafından gösterilecek başka bir sertifika hizmet sağlayıcı tarafından mı yürütüleceği yönetmelikle düzenlenir).

Yönetmelikte devre ilişkin bir hükmün olması gerekir.

Sn. MESUT ORTA'NIN RAPORUNUN DEĞERLENDİRMESİ

Sn. Orta Md. 9 çerçevesinde sertifikaların saklanması hususunu gündeme getirdi ve bununla ilgili yönetmelikte bir düzenlenme yapılaması gerekliliğine işaret etti.

Sn. Orta, elektronik sertifika hizmet sağlayıcılarının sertifikaları 30 yıl süre ile saklamak zorunda olduğu yolundaki görüşünü, grubun bilgisine sundu.

c. Üçüncü Toplantı

29 Haziran 2004 tarihinde saat 14:00'de Telekomünikasyon Kurumunda yapılan toplantıda ise, Hukuk çalışma Gurubunda yeniden bir yapılanmaya gidilmesi kararlaştırılmıştı. Bu yeni Çalışma Gurubu tarafından 5 Temmuz 2004 tarihinde Telekomünikasyon Kurumu'na ilerleme raporu ve sonuç raporu her ikisi birlikte teslim edilecektir.

ALTINCI KISIM – "HUKUK ÇALIŞMA GRUBU SONUÇ RAPORU"

BİRİNCİ BÖLÜM – "5070 SAYILI ELEKTRONİK İMZA KANUNU HAKKINDA GENEL DEĞERLENDİRME"

1. Elektronik İmza Kanununu, Amaç ve Kapsam

Yasa genel yapısı itibariyle Avrupa Birliği'nin 99/93/EC sayılı "Elektronik İmzalarla İlgili Konsey – Komisyon Direktifiyle" uyumludur. Avrupa Birliği ve dünyadaki diğer ülkelerin uygulamaları incelendiğinde, Elektronik İmza Yasalarının genellikle minimalist ve teknoloji yansızlık ilkeleri gözetilerek hazırlandığı görülmektedir. Yasamızın da bu yaklaşımı benimsemesi ve bunun genel gerekçede ifade edilmesi olumludur. Ancak Yasa'nın özellikle Açık Anahtarlı Alt Yapı (Public Key Infrastructure) Teknolojisi ve bu teknolojinin bir açılımı olan "dijital imza"yı düzenlemeyi hedef alan yapısı özellikle kamuoyunda değişik yorumlara neden olmaktadır.

Bu yorumlar, Yasayla ulaşılmak istenen hedeflerin gerçekleştirilmesinde önemli bir direnç noktası teşkil etmektedir. Oysa e-devlet ve e-ticaret uygulamalarına büyük bir ivme kazandıracak temel hareket noktası olan 5070 Sayılı Yasa, doğru bir şekilde kamuoyuna anlatıldığında ve bilimsel gerçekler ışığında yorumlandığında arzu edilen katma değeri yaratmada çok önemli bir misyon yüklenecektir. Yasa genel kurgusu itibariyle bir çok tanımı ve maddeyi Avrupa Birliği'nın 99/93/EC sayılı Konsey – Komisyon Direktifinden alması, Yasa'nın en güçlü yönlerinden biridir. Bu aynı zamanda Avrupa Birliği ülkelerinin uygulamalarından, Direktifin hazırlanış ve uygulanma süreçlerinde ortaya konan zengin bilimsel kaynaklardan yararlanma fırsatının da kapılarını aralamaktadır.

Bu tespitten hareketle Yasanın isminin neden "elektronik imza" yasası olarak belirlendiği, Yasa ile neden belli bir teknoloji (Açık Anahtarlı Alt Yapı – Public Key Infrastructure) üzerinde düzenleme yapılması ihtiyacının ortaya çıktığı bilimsel gerçekler ışığında hiçbir kuşkuya yer bırakılmayacak biçimde açıklığa kavuşturulacaktır. Ancak Yasa'nın gerek genel gerekçesinde gerekse de madde gerekçelerinde bu hususla ilgili ipuçları ve açıklayıcı yorumlar bulunmamaktadır. Bu durum bir çok yönden negatif bir kamuoyu

yaratılarak Yasa'nın yanlış yorumlanmasına ve kendi amacı dışarısında uygulamalar geliştirilmesine yol açabilecek tehlikeleri bünyesinde barındırmaktadır.

Özellikle Yasa'nın Açık Anahtarlı Alt Yapı Teknolojisi üzerinde işlevsellik gösteren dijital imzayı düzenlemeyi hedef alan tutumu, Yasa'nın hazırlanış sürecinde tutarlı ve gerekçeli uygulamaların takip edilmemesi nedeniyle çelişkili bir takım sonuçların Yasayla ortaya konulmasına neden olmuştur. Oysa Birlik düzeyinde bu sorunların aşılması yönünde yeknesaklık ve tutarlılık yaratacak bir çok bilimsel kaynak ve araştırma raporları yayınlanmıştır. Yasa'nın hazırlanış sürecinde bu kaynaklardan ve araştırma raporlarından yeterli derecede istifade edilmediğini de üzülerek gözlemlemekteyiz.

Yasaya kaynaklık eden 99/93/EC Sayılı Direktif ***elektronik imzalarla ilgili temel hukuksal çerçeveyi*** ve ***bu hukuksal çerçevenin en önemli bileşenlerinin statüsünü*** düzenlemeyi hedeflemektedir. Direktif aynı zamanda Birliğin hukuk siyasetini de açıkça ortaya koymakta ve dünyadaki tüm medeni milletlerin de takip ettiği gibi bu siyasetin sonucu olarak belli bir teknoloji hedef alınmaktadır. Bu teknoloji Açık Anahtarlı Alt Yapı Teknolojisidir. Birlik Direktifin düzenlenmesinden önce kamuoyundan aldığı görüşler ve yaptığı hukuksal risk değerlendirmeleri ile Açık Anahtarlı Alt Yapı üzerinde geliştirilen uygulamaların hukuksal bir değer kazanması gerekliliğine karar vermiştir. Birlik bununla birlikte diğer teknolojilerin ve bu alt yapı üzerinde geliştirilebilecek diğer uygulamaların da önünü açmak için Direktif'te teknoloji yansızlık (technology neutrality) yaklaşımının bir ifadesi olarak olarak "elektronik imza"yı çok geniş bir çerçevede tanımlanmıştır. Bu tanım Kanunumuzdaki "elektronik imza" tanımının aynısıdır.

Birliğin elektronik imzalar konusunda neden "Açık Anahtarlı Alt Yapı" yönünde bir tercih belirttiği ise bilimsel verilere ve kantitatif değerlendirme ölçütlerine dayanmaktadır. Açık Anahtarlı Alt Yapı teknolojisi İkinci Dünya Savaşından başlayarak belli bir bilimsel temel üzerine oturtulmuş, 1970'li yılların başından itibaren çok önemli gelişmelerle birlikte giderek yoğun şekilde ticari uygulamalarda kullanılmaya başlanmış, dünya üzerinde standartları ve küresel ölçekte güvenlik ve işlerlilik alanları oluşturulmuş, en güvenilir güvenlik uygulaması olduğu kanıtlanmıştır. Küresel düzeyde bir çok yapı bu teknolojiyi kullanmakta ülkelerin bu teknolojiyle ilgili mevcut ve müstakbel yatırımları bulunmaktadır.

Aynı durum ülkemiz için de geçerlidir. Ülkemizde de gerek devlet gerek özel sektör gerekse de silahlı kuvvetler açık anahtarlı alt yapı uygulamalarını kullanmakta bu konuyla ilgili AR-GE yatırımları yapılmakta ve bu uygulamanın etkin olacağı kullanım ve güvenlik alanları oluşturulmaktadır. Elektronik İmza Kanunu ile "De Facto" durumun hukuksal bir meşruiyete kavuşturulması hukuk siyaseti açısından ve pozitif hukuk öğretisi bakımından en doğru yaklaşımdır. Ancak bu durum net bir biçimde Yasa'nın gerekçesinde açıklanmadığından Kanunkoyucu bir çok haksız eleştiriye maruz kalabileceği gibi, Kanunu uygulamakla görevli olan kurumların da yanlış yöntemler benimsemesine yol açabilecektir.

Yasa, uyumlu olması gözetilen "Direktifte" yer alan belli felsefeleri ve Yasanın "ratio legis"ini teşkil edecek kurgu yapısını da ne yazık ki açıklıkla yansıtamamıştır. Bu durumun nedenleri arasında Yasa'nın hazırlanış aşamalarında karşılaştırmalı hukuk kaynakları arasında maddi hukuk kaynaklarının incelenmesi ancak bunların yaratımında temel teşkil eden uygulamaların, analizlerin ve hedeflerin gözden kaçırılması yatmaktadır. Oysa Yasanın hazırlanış sürecinde karşılaştırmalı hukuktaki maddi hukuk kaynaklarının yanında bu çeşit kaynaklardan da yararlanma sağlansa idi Yasa'nın kurgu yanlışları önlenebilirdi.

Yasayla ilgili detaylı değerlendirmelerimize geçmeden önce açıklığa kavuşturmak istediğimiz bir başka nokta da AAA'nın hukuk politikası olarak bir bilgi güvenliği alt yapısı olarak belirlenmesi ve bu alt yapı üzerinde hukuken elle atılmış imzayla aynı hukuki etki ve sonucu doğuracak olan "dijital imza"ya da "elektronik imza" kanunu çerçevesinde bir değer tanınması hususlarının altı çizilmesidir. Bu tespit özellikle kanunun yorumlanmasında ve yönetmeliklerin hazırlanmasında şu sonuçları gerçekleyecektir;

- ***AAA'nın hukuk politikası olarak bir bilgi güvenliği alt yapısı olarak belirlenmesi***; bu alt yapı üzerinde geliştirilecek uygulamaların, kriptoloji sistemlerinin hukuki çerçevesinin ve bu alt yapının sujeleri bakımından tespit edilecek hukuki sorumluk rejimlerinin AAA'nın işleyişindeki temel dinamikler göz önünde bulundurularak ortaya konulması sonucunu doğurur. Bu durum aynı zamanda ulusal bilgi güvenliği politikalarının ve yatırımlarının da şekillendirilmesinde, uluslar arası entegrasyonun sağlanmasında sektörel ve kamusal yatırımların belli bir şekilde gelişimi için zemin hazırlar.

- ***AAA üzerinde hukuken elle atılmış imzayla aynı hukuki etki ve sonucu doğuracak olan "dijital imza"ya da "elektronik imza" kanunu çerçevesinde bir değer tanınması,*** AAA'nın sadece "dijital imza"ya yönelik olan uygulamaların bir bütün çerçevesinde yorumlanması, kanun ve yönetmelik kapsamında sadece dijital imza'ya yönelik olan değerlendirmelerin dikkate alınması, AAA'nın yorumlamakta temel alınan kriterlerden sadece "dijital imza"ya uyumlu olanların yönetmelik ve kanununun yorumlanması sırasında değer tanınmasını ifade etmektedir. Burada dijital imza olarak ele alınan teknolojinin kanunumuz kapsamında elle atılmış imza ile aynı hukuki statüde sayılan "güvenli elektronik imza"nın teknik ve operasyonel yetkinlikleri karşılaması gerekliliği de hatırdan çıkarılmamalıdır. Bu durum aynı zamanda kanunun ve yönetmeliklerin kapsamının netleştirilmesinde de temel dayanak noktası olacaktır. Yukarıda ifade edilen durumlarla ilgi son olarak ortaya çıkacak sonuç ise imzalama verisi ile şifreleme verisi bir başka ifade ile imzalama anahtar çiftleri (signing key pairs) ile şifreleme anahtar çiftleri (encryption key pairs) arasında gidilecek ayrımda kendinde göstermektedir. Kanun kapsamında güvenli elektronik imza yaratmak amaçlı kullanılacak olan imza oluşturma verisi (private key) aynı zamanda şifreleme amacıyla da kullanılabileceğinden her ikisi arasında teknik bakımından yapılacak ayrım aynı zamanda hukuki sonuçlar da yaratacaktır. Daha açık olarak belirtmek gerekirse hem imzalama hem de şifreleme amaçlı olarak kullanılan veri, imzalama amaçlı kullanıldığında "imza oluşturma verisi" olarak mütalaa edilmeli ve bu kapsam içersinde kanun ve yönetmelikler çerçevesinde ortaya çıkan sonuca bir hukuksal değer tanınmalıdır. Ancak bu veri şifreleme veya başka amaçlarla kullanıldığında, kanun ve yönetmelik kapsamı içersinde değil diğer hukuksal enstrümanlar ve genel hükümler çerçevesinde yarattığı hukuki sonuç tartışmaya açılmalıdır. Bu ayrımın hukuk politikası bakımında yaratacağı sonuçlar çok önemli olduğundan dolayı, Kurum'un yönetmelikleri hazırlarken kullanıcı kolaylığı, tüketiciyi koruma, kaynak israfında bulunulmaması gibi ilkeleri de göz önünde bulundurarak bu durumu açıklığa kavuşturması, kanunun yorumlanması sırasında da bu gerçeğin hatırdan çıkarılmaması gerekmektedir.

5070 sayılı Elektronik İmza Kanununun 1. ve 2. maddelerinde kanunun kapsamı ve amacı açıklanmıştır. Buna göre Kanunun amacı, "elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir". Kanun kapsam olarak, "*elektronik*

imzanın hukukî yapısına, elektronik sertifika hizmet sağlayıcılarının faaliyetlerine ve her alanda elektronik imzanın kullanımına ilişkin işlemlere" işaret etmektedir. Kanunun "Kapsam" başlıklı maddesiyle ortaya konulan elektronik imza kullanımın her alanını kapsaması, sadece dijital imzalara değil her türlü elektronik imzaya *her türlü alanda (kamusal/özel)* hukuki bir çerçeve çizmek amacıyla konulmuştur. Ancak bu durum elektronik imzanın "kapalı bilgisayar ağlarında" iletişim güvenliğini sağlamak için kullanılması durumunda problemler çıkarabilecektir. Elektronik imzaların ve özellikle açık anahtarlı alt yapıyı (AAA) kullanan iletişim sistemlerinin teknik açıdan asıl amacı iletişim güvenliğini sağlamaktır. Günümüzde ağ sistemlerinin çoğu AAA sistemini kullanmaktadır ve bu ağların çoğu kamuya açık ağlar değildir. Örneğin, AAA; bir çok çalışanı olan bir şirkette, şirket çalışanlarının birbirleriyle olan iletişiminin güvenliği, gizli iletilerin sadece yetkili kişiler tarafından görülebilmesi gibi amaçlarla kullanılabilir. Böyle bir sistemde şirketin bir sunucusu (server), çalışanlara sertifika dağıtmak görevini üstlenebilir. Bu sertifikalar kanunda tanımlandığı gibi "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt"lardır. Bu sertifikalar yine kanunda tanımlanan "nitelikli elektronik sertifika"nın gereksinimlerini yerine getirmedikleri takdirde nitelikli sayılmayacaklardır ve bu sertifikalarla atılan imzalar elle atılmış imza ile aynı hukuki değerde olmayacaktır. Ancak bu sertifikaları yayınlayan sunucunun operatörü ve/veya sunucunun sahibi olan kurum; Kanundaki elektronik sertifika hizmet sağlayıcısı tanımının nitelikli/niteliksiz bütün hizmet sağlayıcıları kapsaması sebebiyle, sertifika hizmet sağlayıcılara yüklenen yükümlülüklere tabi olacaktır. Bu yükümlülükler arasında faaliyete başlaması için Telekomünikasyon Kurumuna yapmak zorunda olduğu bildirim de bulunmaktadır. (Md. 8) Bu bildirimde bulunulmazsa, sertifika yayınlayan kişi ve/veya kuruluşlar Md. 17'ye göre "yetkisi olmadan sertifika oluşturmuş" sayılacak ve iki yıldan beş yıla kadar hapis ve bir milyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılabileceklerdir. Sonuç olarak sadece iletişim güvenliği için AAA sistemini kullanan kişi ve kurumlar yukarıda bahsedilen yükümlülüklerle karşı karşıya kalabileceklerdir. Bu sebeple kanunun kapsamına Avusturya'da[1] olduğu gibi kapalı ağ alanları için bir istisna getirilebilir ve bu alanlarda kullanılan elektronik imzanın kanun kapsamında değerlendirilmesi, bu kapalı ağ kullanıcılarının kabul etmesine veya ağ yöneticisinin inisiyatifine bırakılabilir. Bu sakıncaların aşılmasında ve kanunun ruhuna göre

[1] Avusturya Elektronik İmza Kanunu "SigG " md. 1/2

yorumlanmasında en önemli hukuksal enstrüman Telekomünikasyon Kurumu'nun çıkaracağı yönetmelikler olacaktır. Bunun yöntem ve koşullarına ikinci bölümde detaylı olarak değinilmektedir.

2. 5070 Sayılı Kanun'da Tanımlanan Kavramlar

2.1. Elektronik Veri

5070 Sayılı Kanuna göre elektronik veri "*Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar*"dır. Elektronik veri tanımı çoğu yabancı mevzuatta ve Direktif'te yapılmamıştır. Sadece İrlanda[2]'da "elektronik veri" tanımı altında Kanunumuzdakine benzer fakat daha geniş (biometrik, fotonik) bir tanım yapılmıştır. Lituanya[3]'da da "elektronik veri" tanımı enformasyon teknolojisi ile üretilmiş her türlü veri için kullanılmaktadır.

2.2. Elektronik İmza

Kanuna göre elektronik imza "*başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*"dir. Bu tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta genel olarak aynı tanım karşımıza çıkmaktadır. Ancak Direktif'te; kanunumuzda "kimlik doğrulama" olarak belirtilen kısım "tanımlama-authentication" olarak belirtilmiştir. Tanımlama, imza sahibinin kimlik bilgilerini değil veriyi tanımlama olarak algılanmalıdır. Buradan çıkarılması gereken sonuç elektronik verinin elektronik imza sayılması için imza sahibinin kimlik bilgilerini taşıması veya bu bilgileri ortaya koyması gerekmemesidir. Ancak bu koşul ve şartları taşıyan ve bir elektronik veriyi tanımlayan ve ona doğrudan veya dolaylı olarak bağlı olan bir diğer elektronik veri elektronik imza sayılacaktır. Kanundaki "kimlik doğrulama" tanımını daha fazla karşılayan "identify" ibaresi Direktif'te gelişmiş elektronik imzanın (advanced electronic signature) gereksinimleri arasında sayılmıştır(Bkz. 99/93/EC; Md.2/2-b). Bu

[2] İrlanda Elektronik Ticaret Kanunu "Electronic Commerce Act" md.2
[3] Lituanya Elektronik İmza Kanunu md.2/2

sebeplerden ötürü kanunun yorumu yapılırken elektronik imzalarda kimlik bilgilerini doğrulama zorunluluğu aranmamalıdır. Burada açıklanması gereken bir diğer problem, bilgisayar sistemlerinde her türlü tanımlama (authentication) işleminin elektronik imza sayılıp sayılmayacağı ile ilgilidir. Bilgisayar sistemlerinde yapılan tanımlama işlemi "veri tanımlama – data authentication" ve "varlık tanımlama – entity authentication" olarak ikiye ayrılabilir. Veri tanımlama bir verinin doğruluğunun, bütünlüğünün, kaynağının ve bunun gibi özelliklerinin başka bir veri tarafından tanımlanabilmesi işlemidir. Varlık tanımlama ise kullanıcının sisteme kabul edilmesi amacıyla kullanılan tanımlanma yöntemidir. Aradaki ayrımı örneklerle açıklamak gerekirse kullanıcının sisteme girmek için "PIN" kodunu kullanması varlık tanımlama iken, internet üzerinden yapılan bir finans işleminin tanımlanması ise veri tanımlanmadır. Bu tanımlama yöntemlerinden sadece veri tanımlama, 99/93/EC Sayılı Konsey – Komisyon Direktifi'nin altında yatan felsefe çerçevesinde değerlendirildiğinde kanunumuzda açıklanan elektronik imzayı betimlemeye yöneliktir. Kanunda güvenli elektronik imza olarak tanımlanan tanımlama yöntemi AAA sistemi ile çalışan bir tanımlama yöntemidir. Ancak burada unutulmaması gereken bir diğer husus AAA sistemleriyle çalışan bütün tekniklerin veri tanımlama veya başka bir anlatımla elektronik imza olmadığıdır. Zira AAA Örnek olarak Finlandiya'da kullanılan elektronik nüfus cüzdanlarında kullanılan sistem AAA sistemidir fakat bu kartlarla elektronik imza atılabildiği gibi, kart sadece sisteme giriş yani varlık tanımlama amacıyla da kullanılabilir; bu amaçla kullanıldığında burada yapılan işlem elektronik imza olmayacaktır.

2.3. İmza Sahibi

Kanunda imza sahibi "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi" olarak tanımlanmıştır. Direktif'te ve yabancı mevzuatta da bu tanımla örtüşen tanımlar mevcuttur. Burada dikkat edilmesi gereken husus imza sahibinin ancak gerçek kişi olabileceğidir. Ancak yine Kanunun gerekçesinde, sertifikalarda bu hususun açıklıkla belirtilmesi durumunda, tüzel kişiler adına da gerçek kişilerin elektronik imza yaratabilecekleri ve elektronik sertifikaya sahip olabilecekleri belirtilmiştir. Aynı anlama geldiği halde bazı kanunlarda imza sahibi; sertifika sahibi, imza anahtarı sahibi gibi adlarla tanımlanmıştır. Bunlara ek olarak yabancı mevzuatta yapılan tanımlarda imza sahibinin,

imzayı kendi veya temsil etmeye yetkili olduğu bir üçüncü kişi veya kurum adına kullanacağı eklenmiştir. İrlanda[4]'da kamu kurumları da imza sahibi olabilmektedirler. Ayrıca çok doğru bir tanımlama ile Avusturya[5]'da sertifika hizmetlerini sağlamak amacıyla sertifika kullanan sertifika hizmet sağlayıcıları da imza sahibi olarak tanımlanmıştır. Bu isabetli tanımın sebebi, sertifika hizmet sağlayıcıların hizmet sırasında sertifika kullanmak ve kullanıcılara sundukları sertifikaları kendi imza oluşturma verileriyle imzalamak zorunda olmalarıdır. İmza sahibi tanımına böyle bir ek yapılması; imza sahibinin ve sertifika hizmet sağlayıcının yükümlülüklerini, nitelikli elektronik sertifikanın gereksinimlerini belirtirken, bu maddelerde imzalama prosedürü ve imza sahibi ile ilgili hükümlerde karışıklık olmasını engelleyecektir.

2.4. İmza Oluşturma, Doğrulama Araçları ve Verileri

***İmza oluşturma verisi*:** İmza oluşturma verisinin tanımı Kanun'a göre "*İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler*" şeklindedir. Tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta da aynı biçimde tanımlanmıştır. Bu tanım uygulamada "private key" olarak bilinen özel veya kapalı anahtarı belirtmektedir. İmza oluşturma verisinin tanımı teknoloji bağımsız bir yöntemle yapılmıştır. Ancak konuyla ilgili teknik gereksinimler (anahtar uzunluğu, hash değer, rasgele oluşturma kalitesi -random creation quality- v.b.) yönetmelikle düzenlenmelidir. Uygulamada imza oluşturma verisi hem hizmet sağlayıcı tarafından hem de sertifika sahibi tarafından oluşturulabilmektedir.

***İmza doğrulama verisi*:** İmza doğrulama verisinin tanımı Kanun'a göre "*Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler*" şeklindedir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir. Tanım Direktif'in çevirisi şeklindedir ve yabancı mevzuatta da aynı şekilde tanımlanmıştır.

***İmza oluşturma aracı*:** İmza oluşturma aracının tanımı Kanun'a göre *"Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı*"

[4] İrlanda Elektronik Ticaret Kanunu "Electronic Commerce Act" md.2
[5] Avusturya Elektronik İmza Kanunu "SigG "md. 2/2

şeklindedir.. Bu tanımda Direktif'in çevirisidir ve yabancı mevzuatta aynı şekilde tanımlanmıştır. Uygulamada imza oluşturma araçları donanım bazlı olarak akıllı (smart) kartlar, USB Token'lar, bilgisayarlar veya veri işleme kapasitesi olan el terminalleri (PDA, cep telefonları, Pocket PC'ler v.b.) ile yazılım bazlı olarak da ***bilgisayar programları, software smartcard'lar, işletim sistemleri veya özel yazılımlar*** v.b. şeklinde karşımıza çıkabilmektedir.

İmza doğrulama aracı*:** İmza doğruluma aracının tanımı Kanun'a göre "*Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı*" şeklindedir. Bu tanımda Direktif'in çevirisidir ve yabancı mevzuatta aynı şekilde tanımlanmıştır. İmza oluşturma araçları aynı zamanda imza doğrulama araçları olarak da kullanılacağından dolayı burada istisnai olarak sadece imza doğrulama aracı olarak kullanılacak olan donanım ve/veya yazılım bazlı araçların yönetmelik içinde ayrı standartlara referans gösterilerek tanımlanması gerekebilir. Aksi durumda imza oluşturma araçları için belirlenen standartlar imza doğrulama araçlarını da karşılayacağından dolayı bu noktada suni ayrımlara gidilmeye gerek yoktur. Avrupa Birliğinin 99/93/EC Sayılı Direktifinde de bu yaklaşımın bir sonucu olarak güvenli imza doğrulama süreciyle ilgili niteliklerin sayıldığı EK – 4 (Annex – IV) bölümü de ***tavsiye niteliğindedir.

2.5. Zaman Damgası

Kanun'a göre zaman damgası "*Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt*"tır. Direktif'te zaman damgasının tanımı yapılmamıştır. Alman[6] ve Avusturya[7] Elektronik İmza Kanunları'nda yapılan zaman damgası tanımı kanunumuzdaki ile örtüşmektedir. Ancak bu ülkelerdeki elektronik imza düzenlemelerinde tanımlar dışında da zaman damgasının teknik gereksinimleri ve zaman damgası hizmeti veren hizmet sağlayıcıların yükümlülükleriyle ilgili hükümler bulunmaktadır. Kanunumuzda yönetmelikle düzenlenecek hususlar belirtildiği

[6] Alman Elektronik İmza Kanunu SigG md. 2/15
[7] Avusturya Elektronik İmza Kanunu "SigG "md. 2/12

(md.20)'de zaman damgasını düzenleyen hükme bir atıf olmadığından dolayı zaman damgası ***müstakilen*** yönetmelikle ayrıntılı olarak düzenlenemeyecektir. Ancak hizmet sağlayıcıların yükümlülükleri yönetmelikle düzenleneceği için bunlarla birlikte zaman damgası ile ilgili teknik gereksinimler de bu hüküm çerçevesi içersinde ele alınabilir.

2.6. Elektronik Sertifika

Kanun'a göre elektronik sertifika "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt"tır. Bu tanım Direktif'teki ve yabancı mevzuattaki sertifika tanımlarına uygundur. Elektronik sertifikalar; imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü taraf (elektronik sertifika hizmet sağlayıcısı) tarafından teyit edilmesi amacıyla kullanılırlar.

2.7. 5070 Sayılı Kanunda Yer Almayan Ancak 99/93/EC Sayılı Avrupa Birliği Konsey ve Komisyon Direktifinde Geçen Bazı Tanımlar

2.7.1. Elektronik İmza Ürünleri

Direktif'te ve yabancı mevzuatta yer alan bu tanım, sertifika hizmet sağlayıcıları tarafından elektronik imza servisleri için kullanılan veya elektronik imza doğrulama veya oluşturma için kullanılan donanım yazılım ve ilgili bileşenleri belirtmektedir. Buna göre elektronik imza ürünleri Direktif Ek 2/f, 3 ve 4 de yer alan araçlardır. Ek 2/f ve 3'de hizmet sağlayıcıların sertifikasyon hizmeti sırasında kullanacakları araçlar ile imza oluşturma araçlarının gereksinimleri sayılmıştır. Nitelikli sertifika üretmek veya güvenli elektronik imza oluşturmak için burada bahsedilen teknik gereksinimlere uyulması zorunludur. Direktif'in 3/5 md. sine göre Komisyon bu eklerde belirtilen gereksinimlerin yerine geçmek üzere genel olarak tanınmış teknik standartları referans gösterebilir, bu standartları yerine getiren sertifika hizmet sağlayıcıları eklerdeki gereksinimleri yerine getirmiş sayılır. Komisyon bu maddeye dayanarak 13 Temmuz 2003'te aldığı bir kararla bazı standartları

referans göstermiştir. Bu standartlara uyan sertifika hizmet sağlayıcıları ve imza oluşturma üreticileri/dağıtıcıları Ek'lerdeki gereksinimleri yerine getirmiş sayılacaklardır. Komisyon, kararında Avrupa Standardizasyon Komitesi'nin konuyla ilgili standartlarını referans göstermiştir.

2.7.2. İhtiyari Akreditasyon

İhtiyari akreditasyon, sertifika hizmetleri pazarında kaliteyi arttırmak, rekabeti güçlendirmek, sertifika hizmetleri alacak olan kurum ve kişilerin güvenli ürün ve hizmet almalarını teşvik etmek, pazarın giderek güvenlik standartlarını yükseltmekle birlikte tüketicilerin de ürün ve hizmetleri kullanım kolaylığını arttıran bir yöntemdir. İhtiyari akreditasyon, kanuna tabi olan elektronik sertifika hizmet sağlayıcılarının gerek yönetsel, gerek prosedürel gerekse de sunduğu hizmetlerle ilgili kanun haricinde ek gereksinimlerin tanımlandığı ve bu gereksinimleri karşılayan sertifika hizmet sağlayıcıların, akredite eden kurum (özel ve/veya kamusal olarak) tarafından verilen izin gereğince, bu izinde belirtilen hak ve yetkileri kullanmasına imkan tanıyan bir sistemdir. Akredite olabilmek için sertifika hizmet sağlayıcısının, akredite edecek olan kuruma başvurması gerekmektedir. Akreditasyon şartları akredite edecek otorite tarafından kamuoyuna açıklanır. Akreditasyon sadece belirli hizmetlerle ilgili olabileceği gibi sadece bir süreci veya yöntemi kabulle de ilgili olabilir. Akredite edilecek olan hususu (hizmet, ürün, süreç v.b) akreditasyon kurumu açıklayabileceği gibi sertifika hizmetlerinden yararlanmak isteyen herhangi bir kurum veya kişi de talep edebilir. Bu durum akreditasyonun genel yapısını uygundur. Ancak sertifika hizmet sağlayıcı pazara yeni süreceği bir hizmet, ürün veya süreçle ilgili bir akreditasyon talep ettiği takdirde bu durum daha çok bir kalite veya uygunluk denetimi yapmak olarak yorumlanabilir. Her iki durum da ihtiyari akreditasyon çerçevesinde mütalaa edilmektedir. Akredite eden otoriteden akredite edilen hususlarla ilgili belge alan sertifika hizmet sağlayıcı, bu hususlarla ilgili spesifik hizmetleri yürütmek adına bir yetki olmuş olur. Örneğin elektronik imzayla ilgili düzenlemelerde tanımlanan anahtar uzunluğundan daha yüksek bir anahtar uzunluğu veya kanunda tanımlanan sertifikaların nitelikleri yanında farklı niteliklerin de arandığı bir sertifikasyon hizmeti almak isteyen bir kurumun bu isteğinde belirttiği hususlarla ilgili ancak bu hususlara uygunluğu akreditasyon otoritesi tarafından tanınmış sertifika hizmet sağlayıcıları yerine getirebilir. Kanunumuzda ihtiyari akreditasyona yer verilmemesi

elektronik imzanın aynı zamanda bir güvenlik teknolojisinin bileşeni olduğu hususu da göz önünde bulundurulduğunda, kanundaki nitelikleri karşılamasına rağmen farklı nitelikleri de bünyesinde barındıran hizmet, ürün ve süreçlerin dışlanma tehlikesini yaratabilecek bir duruma işaret etmektedir. Bu durum gerek kanunu yorumlayanlar gerekse de Kurum tarafından ortaya konulacak düzenlemeler ve uygulamalar bakımından Yüksek Mahkemenin "Çoğun içersinde, azda vardır" şeklinde ifade ettiği veya "*quando plus fit quam fieri debet, videtur etiam illut fieri quod faciendum est - yapılması lazım gelenden fazla yapılmışsa yapılması gerekli olan kısım da yapımlı sayılır*" şeklinde açıklanan hukukun genel ilkelerine dayanarak çözüm getirebilir.

Alman Dijital İmza Kanunu'nun ihtiyari akreditasyonla ilgili hükümlerine göre; yetkili otorite başvuru üzerine hizmet sağlayıcıları akredite edebilir. Kurum akreditasyon araştırması için özel kurumları kullanabilir. Akredite edilen hizmet sağlayıcılara Akreditasyon Kurumu tarafından "kalite belgesi" verilir. Bu kalite belgesi, hizmet sağlayıcının hizmetlerinin teknik ve idari olarak test edildiğini göstermektedir. Elektronik Sertifika Hizmet Sağlayıcısı bu kalite belgesi ile kendisini akredite edilmiş bir hizmet sağlayıcı olarak kamuoyuna duyurabilir. Akredite edilmiş olan hizmet sağlayıcılarının sürekli olarak test edilmeleri ve kanunda belirtilen nitelikleri sağlayan araçları kullanmaları gerekir. Bu testler sırasında akredite edilmiş hizmet sağlayıcısı vasfını kaybeden hizmet sağlayıcı elindeki sertifikaları başka bir akredite edilmiş sağlayıcıya veya yetkili kuruma devretmek zorundadır.

Uygulamada ihtiyari akreditasyon, akreditasyon şemaları ile yapılmaktadır. Sağlayıcılar yetkili kurumlara kendilerini akredite ettirmekte ve bu şemalara kendilerini kaydettirmektedirler. Hollanda'da TTP.NL, İngiltere'de T-Scheme, İsveç'te SWEDAC tarafından yetkilendirilen kuruluşlar akreditasyon otoritelerine örnek olarak gösterilebilirler. Ayrıca İhtiyari Akreditasyon Şemaları Grubu (VİTAS) da akreditasyonla ilgili çalışmalarını sürdürmektedir.

3. Güvenli Elektronik İmza, Hukuki Sonuçları, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

3.1. Güvenli Elektronik İmza

Kanuna göre;

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 imzalar güvenli elektronik imzadır." Güvenli elektronik imzaların önemi elle atılmış imza ile aynı hukuki sonucu doğurmalarıdır. Yabancı mevzuatta bu hukuki etkiye sahip elektronik imzalar çeşitli adlarla (nitelikli, evrensel, elektronik imza v.b.) ve farklı teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, ***nitelikli elektronik sertifikaya dayanarak ve güvenli elektronik imza oluşturma aracıyla oluşturulmuş olmalarıdır***. Kanunda yapılan tanımda, Direktif Md. 2/2-a'da belirtilen gelişmiş elektronik imza (advanced electronic signature) tanımında belirtilen bazı gereksinimler ile Md. 5/1'de belirtilen gereksinimlerin birleştirilmesi sonucu oluşturulmuştur. Böylece Direktif'in ortaya koyduğu elektronik imza sınıflandırılmasından (elektronik imza {electronic signature}, gelişmiş elektronik imza {advanced electronic signature}, elle atılmış imza ile aynı hukuki etkiye sahip imza olan nitelikli elektronik imza {qualified electronic signature}) ayrı bir sınıflandırılmaya gidilmiştir. Kanunumuzda sadece elektronik imza ve güvenli elektronik imza ayrımı vardır.

3.2. Güvenli Elektronik İmzanın Hukuki Sonuçları

3.2.1. Elle Atılmış İmza İle Aynı Hukuki Sonuçları Doğurması

Kanun'a göre "*Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur*". Bu hüküm Direktif Md 5/1'ine uygundur. Direktifteki Md. 5/1'e göre nitelikli sertifikaya dayanan ve güvenli imza oluşturma aracı ile oluşturulan imzaların hukuki etkisi elle atılmış imza ile aynı olmalıdır ayrıca bu imzanın delil niteliği inkar edilmemelidir. Yabancı mevzuatta elektronik imzanın hukuki değerinin farklılık arz ettiği görülmektedir. Alman Elektronik İmza Kanunu'nda elektronik imzanın hukuki sonuçları ile ilgili bir hüküm bulunmamaktadır. Alman Mevzuatında, elektronik imzanın hukuki sonuçları genel hükümleri düzenleyen diğer mevzuat (Medeni Kanun, Medeni Usul Kanunu) içersinde düzenlenmektedir. Bulgar Elektronik İmza Kanunu'nda ise normal, nitelikli ve evrensel elektronik imza çeşitleri bulunmaktadır. Bunlardan nitelikli elektronik imza özel hukuk kişileri arasında elle atılmış imza ile aynı sonucu doğururken, evrensel elektronik imza kamu kurumları ve gerçek kişiler arasında elle atılmış imza ile aynı hukuki sonucu doğurur. Evrensel elektronik imzanın nitelikli elektronik imzadan farkı kullanılan sertifikaların akredite edilmiş bir hizmet sağlayıcı tarafından sağlanıyor olmasıdır.

3.2.2. Elektronik İmzanın Delil Niteliği

Kanunun 23. maddesi ile Hukuk Usulü Muhakemeleri Kanunu'nun (HUMK) 295. maddesine eklenmesi kararlaştırılan 295/A maddesinin birinci fıkrasında "***güvenli elektronik imza"*** ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar" denilmektedir. Güvenli elektronik imza ile imzalanmış belgeyi senet ve aksi ispat edilinceye kadar kesin delil kabul edileceğini tespit eden bu madde, hakimin takdir yetkisini kısıtlaması yönünde tenkit edilebilir ise de Birleşik Devletler'de bir çok eyalet elektronik imza ile imzalanmış belgeleri kesin delil olarak kabul etmekte ve bunların ispat kuvvetini de kesin delil olarak sayılan diğer delillerden daha üstün tutmaktadır. Bu hükümlerin ***ratio legis***'i hukuk politikası açısından değerlendirildiğinde, elektronik imza kullanımının yaygınlaştırılması ve elektronik ortamda yapılan işlemlerin teşvikidir. Bilgi çağına giden yolda, bireylerin elektronik ortama daha fazla güven doğmasını sağlamayı amaçlayan bu yaklaşım, hukuk sistematiğimiz açısından tartışılabilir ise de devletin hukuksal düzenleme yolu ile teknoloji kullanımını teşvik etmenin güzel bir örneğini de oluşturmaktadır.

Elektronik imzanın delil niteliğiyle ilgili duruma açıklık getiren Direktif'in 5/2 Md.'sine göre üye devletler, *elektronik imzanın*;

a) *Elektronik biçimde olması*
b) *Nitelikli sertifikaya dayanmaması*
c) *Akredite edilmiş bir sertifika hizmet sağlayıcının sağladığı sertifikaya dayanmaması*
d) *Güvenli elektronik imza oluşturma aracı ile oluşturulmamış olması*

nedenlerinden biri sebebiyle delil niteliğini yadsıyamazlar. Direktif'in bu hükmü Kanunumuza alınmamıştır. Elektronik imzanın delil değerini sadece güvenli elektronik imza ile sınırlamak bir hukuk politikası yaklaşımı olsa da güvenli elektronik imza dışındaki elektronik imzalara da kesin delil değerinde olmasa bile delil niteliği tanımak direktifin bu maddesinin amaçlarına uygun düşmektedir. Örneğin Avusturya[8]'da olduğu gibi, HUMK 295/A maddesine güvenli elektronik imza olarak kanunun aradığı niteliğe sahip olmayan elektronik imzaların da delil niteliğinin inkar edilemeyeceği madde metnine eklenebilir.

3.2.3. Elektronik İmza ile Yapılamayacak Hukuki İşlemler

Kanun'un 5. Maddesinin 2. Fıkrası uyarınca "*Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez*". Güvenli elektronik imzanın uygulama alanın gösterildiği bu maddeye göre noterlerin yapacağı işlemler, noterlerin huzurunda yapılan işlemler, resmi bir makamın katımını veya tescil zorunluluğu gerektiren işlemler (gayrimenkul, motorlu araç alım satımı v.b.) ile evlenme gibi resmi memur önünde gerçekleştirilmesi zorunlu olan hukuki işlemler güvenli elektronik imza ile yapılamazlar. Kanun metninde güvenli elektronik imza ile yapılamayacak hukuki işlemlerin genel bir ifadeyle tanımlanması bazı karışıklıklara sebebiyet verebilecektir. Özellikle doktrinde tartışmalı olan "*teminat sözleşmeleri*" türleri ile "*kanunun özel bir merasime tabi tuttuğu hukuku işlemler*" uygulamada tereddüt yaratacak en önemli hususlardır. Bunların yerine Avusturya[9]'da olduğu gibi elektronik imza kullanarak

[8] Avusturya Elektronik İmza Kanunu "SigG "md. 3/2
[9] Avusturya Elektronik İmza Kanunu "SigG "md. 4/2

yapılamayacak olan hukuki işlemlerin açıklıkla sayılması uygulamada kolaylık sağlayacaktır. Bunun yanında Amerika Birleşik Devletlerindeki elektronik imzalarla ilgili Federal Düzenleme'nin *Özel İstisnalar "* kenar başlığını taşıyan Bölüm 103/c *"İstisnaların Yeniden Gözden Geçirilmesi"* konusunu düzenlemektedir. Bu hükme göre; Haberleşme ve Enformasyon Bakan Yardımcısı aracılığıyla hareket eden Ticaret Bakanı, üç yıllık süre içinde, elektronik imzanın kullanılamayacağı hukuki işlemler olarak gösterilen istisnaların tüketicilerin korunması için gerekli olmaya devam edip etmediğini değerlendirmek için alt bölüm a ve b'deki istisnaların işleyişini yeniden gözden geçirecektir. Birleşik Devletlerdeki bu düzenlemeye paralel olarak 5070 Sayılı Kanuna güvenli elektronik imza kullanarak yapılamayacak olan hukuki işlemlerin belirli bir resmi makamın (Örneğin Bakanlar Kurulu'nun) kanunda belirlenen süreler içersinde kanunda işaret edilen resmi makamın takdirine bağlı olarak değiştirilebileceği hükmünü dahil etmek isabetli bir yaklaşım olacaktır. Zira teknolojideki ilerlemeler; özellikle resmi makamların sunduğu hizmetlerin gün geçtikçe elektronik ortamdan da verilebiliyor olması gerçeği, bugün itibariyle çeşitli saiklerle güvenli elektronik imza kullanarak yapılamayacak olan hukuki işlemlerin ilerleyen zamanlarda alt yapısı oluşsa bile kanundaki emredici hükmün bir gereği olarak yine klasik usullerle gerçekleştirilmesini zorunlu kılacaktır. Bu nedenle kamu yararı, toplumsal ve teknolojik uygunluk takdirini yapabilecek olan bir kamusal otoriteye kanunda yetki tanınarak, kanunda belirtilen güvenli elektronik imza ile yapılamayacağı belirtilen hukuki işlemlerin belirli bir süre içersinde eğer toplumsal ve teknolojik uygunluk açısından kamu yararı da bunu gerektiriyorsa kanun kapsamı içersine alınmasının bu makamın kararı ile sağlanması uygun bir yöntem olacaktır.

3.3. Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

5070 sayılı Elektronik İmza Kanunu'nda, güvenli elektronik imza oluşturma ve doğrulama araçlarının özellikleri sayılmıştır. Burada belirtilen özelllikler Direktif'in Ek - 3 ve EK- 4 bölümlerinde belirtilen niteliklerin ve durumların tercümesidir. Direktif'te ***güvenli elektronik imza doğrulama süreçlerinin nitelikleri*** gereklilik (requirement) olarak değil tavsiye (recommendation) olarak belirtilmiştir. Bu durumun yansıması karşılaştırmalı hukukta bazı ülke kanunlarında ***doğrulama araçlarının niteliklerinin gereksinim bazılarında ise tavsiye olarak sayılmasına*** neden olmuştur. Bu durum Direktifin EK - 4 bölümünün

karşılaştırmalı hukuktaki kanun koyucular tarafından yanlış yorumlanmasının bir sonucudur. Zira elektronik imza oluşturma aracı olarak kullanılan donanım ve/veya yazılımlar aynı zamanda elektronik imza doğrulama amaçlı olarak da kullanılmaktadır. Direktifte, elektronik imza doğrulama sürecinin niteliği tavsiye niteliğinde açıklanmaktır. Bu durum elektronik imza doğrulama süreçlerinin teknolojideki değişiklikler ve tüketicilerin ihtiyaçları doğrultusunda sürekli değişebilmesi nedeniyledir. Kanunkoyucu, 5070 Sayılı Kanunda güvenli elektronik imza doğrulama araçlarıyla ilgili yönetmelik çıkarılacağı noktasında bir hüküm sevk ederek, karşılaştırmalı hukuktaki bazı kanunkoyucuların düştüğü yanlışa kapılmıştır. Burada doğru olan yaklaşım Direktif'in ortaya koyduğu tavsiye yaklaşımıdır; Çünkü imzayı doğrulayan kişiler yani alıcılar imzalama sisteminde pasif konumdadırlar. Alıcıların ne imza sahipleriyle ne de hizmet sağlayıcı ile sözleşmeden kaynaklanan bir hukuki ilişkileri ve yükümlülükleri yoktur. Bu sebeplerden ötürü doğrulama aracını kullanan alıcıya böyle bir yükümlülük yüklemek doğru olmayacaktır ayrıca elektronik imza kullanımının yaygınlaşmasını engelleyecektir. Doğrulama araçlarının belirtilen nitelikleri tavsiye olarak görülmeli ve bu araçları üreten/dağıtan sujelerin imza oluşturma araçları için öngörülen standartları yerine getiren ürünleri piyasaya sunmaları sağlanmalıdır.

Dünyadaki elektronik imza düzenlemeleri, teknik gereksinimlerle ilgili hükümlerde uluslar arası ölçekte standartları belirleyen kuruluşlarının standartlarını referans göstermektedir. Bunun sebebi elektronik imzalar ve bu imzalarla ilgili alt yapının sınırlar ötesi yapısıdır. Bu yapı sayesinde elektronik imza sahibi imzasını pek çok ülkede kullanabilir. Ancak yerel imza düzenlemeleri arasındaki farklılıklar bu yaygın kullanımının önüne geçmektedir. Uluslararası standartların referans gösterilmesi, referans gösteren ülkelerde teknik gereksinimlerle ilgili olarak ortak bir yapı ortaya koymaktadır. Böylece imzanın sınır ötesi kullanımının önündeki engellerin bir kısmı ortadan kalkmış olacaktır. Standart referans gösterme ile ilgili bir diğer sebep ise bu teknik gereksinimlerin belirlenmesi için ortaya konması gereken çalışmanın mali külfetidir.

Dünyadaki elektronik imza düzenlemelerinde RFC, COBIT, CEN, ETSI, FIPS, ITSEC gibi standartlar referans gösterilmektedir. Konuyla ilgili yönetmelikler düzenlenirken bu standartlar araştırılmalı ve bunlar referans gösterilerek düzenleme yapılmalıdır.

Güvenli elektronik imza oluşturma ve doğrulama araçları, Direktif EK- 2/f'de belirtilen sertifika hizmet sağlayıcının sertifika hizmetleri için kullanacağı araçlarla birlikte elektronik imza ürünleri olarak da adlandırılmaktadırlar. Direktif Md. 3/5 göre Komisyon elektronik imza ürünleri için uluslararası standartları referans gösterebilir ve bunları Avrupa Birliği Resmi Gazetesinde yayınlayabilir. Güvenli elektronik imza oluşturma araçları (Direktif EK-3) ve sertifika hizmet sağlayıcının kullanacağı araçlarla (EK-2/f) ilgili yayınlanan standartlarda belirtilen gereksinimleri yerine getiren hizmet sağlayıcıları, üreticiler ve satıcılar Direktif'in eklerinde belirtilen gereksinimleri yerine getirmiş sayılacaktır. Direktif'e göre üye devletler de bu standartları yerine getirenlerin, güvenli elektronik imza oluşturma aracı ve hizmet sağlayıcıların kullanacağı araçlarla ilgili gereksinimleri yerine getirdiklerini kabul edeceklerdir.

Komisyon 14 Temmuz 2003 de aldığı bir kararla Direktif Ek - 2/f ve EK-3 de belirtilen gereksinimler ile ilgili olarak standartların referans numaralarını yayınlamıştır. Buna göre EK - 2/f de belirtilen gereksinimler için CEN CWA 14167-1 ve CEN CWA 14167-2; EK - 3'te belirtilen gereksinimler için CEN CWA 14169 standart olarak belirlenmiştir. Burada açıklığa kavuşturulması gereken bir başka husus da Direktifin EK- 2/f' maddesinde belirtilen 5070 Sayılı Kanunun 8. Maddesinin 2. Fıkrasının (a) Bendinde altı çizilen "güvenli ürün ve sistemleri" oluşturun araçların hacze konu olması hususudur. Bu araçlar haczedildiği zaman elektronik imza ve sertifikalarla ilgili hizmet sağlayıcının yaptığı bütün işlemler duracaktır. Bu sebeple bu araçlar ya haczi kabil olmayan mallardan sayılması ya da hacze konu olmaları halinde sertifika hizmet sağlayıcının elindeki sertifikaları başka bir sağlayıcıya devretmesi imkanı ve zorunluluğu tesis edilmelidir.

Elektronik imza ürünleri yönetmelikle ayrıntılı olarak düzenlenirken bu standartların referans gösterilmesi gerekmektedir. Avrupa Birliği uyum süreci içerisinde düzenlemelerini yeniden gözden geçiren Türkiye, üye devletlerin uymak zorunda olduğu standartları benimsemeli, bu standartları aynı zamanda Türk Standardı haline de getirerek konuya düzenlemelerinde yer vermelidir. Ayrıca elektronik imza ürünleri dışında CEN'in elektronik imza süreçleri ile ilgili olarak pek çok standardı bulunmaktadır. Diğer konularda da düzenleme yaparken CEN'in standartlarına değer tanımak elektronik imzanın uluslararası kullanımını kolaylaştıracaktır.

4. 5070 Sayılı Kanunda Tanımlanan Sertifika Türleri ve Elektronik Sertifika Hizmet Sağlayıcısı

4.1. Elektronik Sertifika ve Nitelikli Elektronik Sertifika

Nitelikli elektronik sertifikalar, kanunlar veya yönetmeliklerle nitelikleri belirlenmiş olan elektronik sertifikaların bu özelliklerine ek olarak bazı teknik gereksinimleri sağlayan ve sertifika sahibinin kişisel bilgilerini içeren elektronik sertifika türüdür. Direktif'in EK -1 numaralı bölümünde nitelikli sertifikanın şartları sayılmıştır. Avrupa Birliği normlarını esas alan ülkelerin düzenlemelerinde ve Kanunumuzda nitelikli elektronik sertifika tanımı Direktif'in EK-1 bölümünün çevirisi şeklindedir. Ancak karşılaştırmalı hukukta genellikle nitelikli elektronik sertifika tanımı yapılırken, sertifikanın nitelikli elektronik sertifika verme şartlarını yerine getirmiş bir hizmet sağlayıcı tarafından verilmesi zorunluluğu getirilmiştir[10]. 5070 Sayılı Kanunda böyle bir zorunluluk bulunmamaktadır. Bu şekilde bir ekleme hem hangi sertifikaların nitelikli sertifika olduğunu anlamayı kolaylaştıracak hem de kanundaki nitelikli elektronik sertifikaların özelliklerini taşımayan elektronik sertifikaları yayınlayan hizmet sağlayıcı ile nitelikli sertifika yayınlayan hizmet sağlayıcının farklı yükümlülüklere tabi olmasını sağlayacaktır. Karşılaştırmalı hukukta ve kanunumuzda Direktif'ten farklı olarak, nitelikli elektronik sertifikada eğer varsa vekalet yetkisine ilişkin bilginin de bulunması zorunludur. 5070 Sayılı Kanunda nitelikli elektronik sertifikanın özellikleri arasında sayılan bir başka husus da sertifikanın eğer varsa limitlerinin (maddi sınırlamalarının) sertifikada bulunması zorunluluğudur. Kanunun 13. maddesine göre de elektronik sertifika hizmet sağlayıcı sertifikanın kullanım ve maddi kapsamına ilişkin sınırların dışında, hiçbir şekilde sorumluluğunu sınırlayamaz. Uygulamada sertifikalar imza sahibine sağlanırken sertifikanın kullanılacağı işlemlerdeki maddi sınır belirlenebilir. Eğer imza sahibi sertifikayı bu sınırların üstünde bir işlemde kullanırsa elektronik sertifika hizmet sağlayıcı bu sınırın üstünde yapılan işlemlerden doğan zararlardan sorumlu değildir. Bununla birlikte sertifikanın kullanımı bazı işlemlerle de sınırlandırılabilir (bankacılık işlemleri,

[10] Avusturya Elektronik İmza Kanunu "SigG "md. 2/3 - 7

güvenli e-posta v.b.). Sertifikanın bu işlemler dışında kullanılması da hizmet sağlayıcının sorumluluğu dışında kalacaktır.

Nitelikli elektronik sertifikanın özelliklerini sıralayan Md. 9'un (j) bendine göre "*Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan **güvenli elektronik imzasının***" sertifikada bulunması zorunludur. Ancak güvenli elektronik imza ve imza sahibi tanımlarına göre; kanunda imza sahibinin ancak gerçek kişi olabileceği belirtilmiştir. Bu durumda hizmet sağlayıcı sadece gerçek kişi olabilir gibi bir sonuç ortaya çıkarmaktadır. Bu sorunun giderilmesi için "imza sahibi" tanımına Avusturya[11]'da olduğu gibi "sertifika hizmetlerini sağlamak üzere sertifika sağlayan hizmet sağlayıcılar"nın da eklenmesi gerekmektedir.

Nitelikli sertifikalarla ilgili özellikler Direktif, karşılaştırmalı hukuktaki düzenlemeler ve Kanunumuzda sayılan hususlarla sınırlı değildir. Bu nedenle pek çok ülke elektronik imza ile ilgili düzenlemelerinde uluslararası standartları referans göstererek (Örn. X.509 v 3, ETSI v.b.) nitelikli elektronik sertifikalar için aranan özelliklerin dinamik bir çerçeveye kovuşmasını sağlamıştır.

4.2. Elektronik Sertifika Hizmet Sağlayıcı

Kanun'a göre elektronik sertifika hizmet sağlayıcıları "*elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir*". Kanunda yapılan tanım Direktif'e uygundur ancak hizmet sağlayıcının yüklendiği sorumluluklar düşünüldüğünde bu tanım oldukça geniş bir tanımdır. Sertifika hizmeti sağlamak, kanunda yapılan tanımın da desteklediği şekilde sadece bilgisayarlar aracılığıyla yapılan bir işlemdir. Açık anahtarlı altyapı sistemiyle çalışan bir bilgisayar ağında, bilgisayar kullanıcıları iletişimlerini güvenli hale getirmek için sertifikalar kullanabilirler ve bu durumda sistemdeki güvenlik sunucusu (server) sertifika ve zaman damgası hizmeti sağlar. Kanuna göre bu sunucunun operatörü veya sunucunun sahibi olan

---

Almanya Elektronik İmza Kanunu "SigG "md. 7

[11] Avusturya Elektronik İmza Kanunu "SigG "md. 2/2

kişi veya kurum "sertifika hizmet sağlayıcısı" olacak ve sağlayıcıya ait yükümlülüklere (kuruma bildirim, denetim, yönetmelikle getirilecek ek yükümlülükler) tabi olacaktır. Böyle bir durumun oluşmaması için kanunkoyucu 20. Madde kapsamında düzenlenecek yönetmeliklerle Telekomünikasyon Kurumuna yetki tanımıştır. Burada kritik olan husus Kanunun lafzıyla bağlantılı olarak "*elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetlerin"* Kurum tarafından hazırlanacak olan yönetmelikte elektronik sertifika hizmeti hizmet sağlayıcı olmak için gerekli yatırımları, alt yapıyı ve nitelikli insan gücünü bir araya getirmiş olan kurumlara yönelik olarak tanımlanmasıdır. Böyle bir yöntem kanunun amaç dışında yorumlanmasını engelleyeceği gibi, *"ilgili hizmetlerin"* kavuşturulmasıyla da sertifikasyon pazarına girecek olan oyuncuların yapacakları yatırımları öngörerek bu piyasaya girmeleri sağlanacak ve böylelikle tüketicileri koruyan bir felsefe ile elektronik sertifika hizmet sağlayıcısı olmak için belli bir nitelik eşiğini de yaratılacaktır. Kurum, "ilgili hizmetlerin" tanımlanmasında AICPA/CICA "Web Trust Program For Certification Authorites" ile ETSI'nin "Sertifika Hizmet Sağlayıcıları Operasyonları" ile ilgili belgelerinden yararlanabilir.

Kanun'a göre "*Elektronik sertifika hizmet sağlayıcı Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer*". Direktif Md. 3/1'e göre de elektronik sertifika hizmet sağlayıcıların kurulması ve/veya faaliyete geçmesi izne tabi tutulamaz. Direktifte yer alan bu prensip Avrupa Birliği'ne üye olan ülkelerde genellikle benimsenmiştir. Bildirim zorunluluğu, yabancı ülkelerde farklı uygulamalarla karşımıza çıkmaktadır. Kimi ülkelerde tüm sağlayıcılar bildirimde bulunmak zorundayken, kimilerinde sadece nitelikli elektronik sertifika sağlayanlar bildirimde bulunmak zorundadırlar. Bazı ülkelerde ise akredite olmak isteyen sağlayıcılar ayrıca bildirimde bulunmak zorundadırlar. Bildirim bedelleriyle ilgili uygulamada da farklılıklar bulunmaktadır. Bedeller sertifika başına veya senelik olarak çeşitli kıstaslara göre belirlenebilmektedir. Yönetmelikle bildirimin niteliğini ve kapsamını belirleyecek olan Telekomünikasyon Kurumu bildirimde istenecek olan belgeleri ve kapsamı objektif kriterlere dayanarak geniş tutarak pazara giriş koşullarını belli bir nitelik eşiğine yükseltebilir. Böylelikle Kurum "ex – ante" olarak asli fonksiyonlarından biri olan sertifikasyon hizmetleri pazarını düzenlemek görevini bir ölçüde yerine getirmiş olacaktır.

5. Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri ve Hukukî Sorumluluğu

5.1. Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri

5070 sayılı Elektronik İmza Kanunu'nun 10. maddesinde sertifika hizmet sağlayıcılarının yükümlülükleri belirtilmiştir. Madde Direktif'in nitelikli elektronik sertifika sağlayan sertifika sağlayıcılarla ilgili özellikleri belirleyen EK - 2 bölümü ile uyumludur. Ancak Direktifin EK-2 bölümünün isminden de anlaşılacağı üzere burada belirtilen yükümlülükler ***nitelikli elektronik sertifika*** sağlayan hizmet sağlayıcılara ilişkindir oysa Kanunumuzda bu yükümlülükler ilk bakışta tüm hizmet sağlayıcılar için öngörüldüğü söylenebilir. Ancak Md. 8'in uygulanmasına yönelik olarak Kurum tarafından çıkarılacak yönetmelikte bu durumun Direktif hükümlerine uyumlu olarak düzenlenmesi için çok önemli bir hukuki dayanak bulunmaktadır. Bu hukuki dayanak Kurumun "ilgili hizmetler" kavramına açıklık getirmek zorunluluğunda yatmaktadır. Kurum "elektronik sertifika hizmet sağlayıcılarının elektronik imza, elektronik sertifika ve zaman damgası ile ilgili sağladığı hizmetlerden" elektronik sertifikaya ilişkin olan hizmetleri yönetmelik içinde tanımlarken, bunlardan birisinin "nitelikli elektronik sertifika üretmek" olarak belirterek, sadece nitelikli elektronik sertifika üreten gerçek ve/veya tüzel kişileri elektronik sertifika hizmet sağlayıcıları olarak mütalaa edilmesini sağlayabilir.

Madde 10'a göre, Elektronik sertifika hizmet sağlayıcısı aşağıdaki yükümlülükleri yerine getirmekle yükümlüdür.

a) Hizmetin gerektirdiği nitelikte personel istihdam etmek

Burada bahsedilen personelin niteliği iki aşamalıdır. Personel görev alacağı pozisyona uygun olarak bilgisayar bilimleri, kriptoloji, elektronik imza, programlama, açık anahtarlı alt yapı, ağ sistemleri ve sertifikasyon konularında yeterli teknik bilgi, tecrübe ve beceriye sahip olmalıdır. Bunun yanında çalışan personelin belli suçlardan dolayı hüküm giymemesi ve yüksek derecede gizlilik ve güvenlik isteyen görevlere üstlenecek olan kişilerde aranan kişisel

özelliklere de sahip olması gerekmektedir. Elektronik Sertifika Hizmet Sağlayıcısı personelinin bu niteliklere sahip olduğunu Kurum'a yapacağı bildirimde tevsik etmelidir.

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

Elektronik sertifika hizmet sağlayıcı nitelikli sertifika talebinde bulunan kişiye sertifika sağlamadan, bu kişinin beyan ettiği kimlik bilgilerinin gerçeğe olan uygunluğunu resmi belgelere göre güvenilir bir biçimde tespit etmekle yükümlüdür. Kurumun çıkaracağı yönetmelikle açıklığa kavuşturulacak olan iki husus vardır. Bunlardan ilki "***kimlik bilgileri***" kavramıdır. Avrupa Birliği'nde "kimlik bilgileri" kavramı üzerinde uzlaşılmış olan dört tür bilgi vardır. Bu bilgilerin seçilmesinde temel alınan kriter bu dört bilginin birlikte kişiyi herhangi bir karışıklığa neden olmayacak biçimde tanımlayabilme kabiliyetidir. Bu bilgiler "kişinin ad ve soyadı", "kişinin doğum yeri", "kişinin doğum tarihi" ve "vatandaşlık kimlik numarasıdır". Ülkemizde de Kurumun yapacağı düzenlemelerde bu dört bilginin doğrulanması kişinin kimliğini tespit etmekte yeterli olarak görülmelidir. Kurumun çıkaracağı yönetmeliklerde açıklığa kavuşturulacak olan ikinci unsur ise kişinin kimliğinin ***"resmi belgelere göre güvenilir biçimde tespit etmek"*** hususudur. Kurum yukarıda saydığımız ve kimlik bilgilerini oluşturan hususları yine yönetmelikte belirleyeceği resmi belgelere dayanarak tevsik edilmesini aramalıdır. Bu resmi belgeler nüfus cüzdanı, pasaport veya eşdeğer nitelikteki herhangi bir resmi belge olarak tanımlanabilir. Burada tartışmaya açılması gereken ve Kurum tarafından kural ve koşulları tespit edilecek bir diğer hususta kimlik bilgilerinin resmi belgelere dayanarak ***güvenilir*** bir biçimde tespit edilmesi hususudur. Yönetmelikle netleştirilecek olan husus güvenilirliğin nasıl sağlanılacağı noktasında toplanmaktadır. Avrupa Birliğinde özellikle ETSI bünyesinde yapılan çalışmalarda nitelikli elektronik sertifika alma talebinde bulunan kişinin bu başvurusu sırasında bildirdiği bilgilerin doğrulunun doğrudan veya dolaylı yöntemlerle yapılabilmesine cevaz verilebileceği belirtilmektedir. Doğrudan yapılacak doğrulama yönteminde kişi başvuruyu yaparken yukarıda bahsi geçen resmi belgelerin asıllarını da ibraz etmektedir. Evrak üzerinden yapılan inceleme sonucunda kişinin verdiği kimlik bilgilerinin doğrulanması yapılmaktadır. Dolaylı olarak yapılan doğrulama yönteminde ise nitelikli elektronik sertifika almak isteyen kullanıcının kimlik bilgileri güvenilir veritabanlarında tutulan bilgilerle karşılaştırılarak

yapılmaktadır. Burada güvenilir veritabanlarında sorgulama yapmaya elverişli bilgilerin kullanıcı tarafından sertifika hizmet sağlayıcısına veya kişi adına nitelikli elektronik sertifika alma talebinde bulunacak olan kuruma bildirilmesi yeterli olmaktadır. ETSI'nin çalışmalarında bu bilgiler "banka hesap numarası", "pasaport numarası", "kişinin çalıştığı kurum tarafından kendisine verilmiş olan gizlilik niteliğine haiz olan çalışan numarasıdır". Dolaylı yoldan yapılan doğrulama için bu bilgilerin verilmesi yeterli olmakta, böylelikle nitelikli elektronik sertifikaların dolayısıyla elektronik imza kullanımın yaygınlaşmasının yolu açılmaktadır. Bu durumun pratikte ve Kurumun düzenleyici yönetmelik nezninde doğuracağı hukuki sonuçlar kurumsal olarak toplu bir biçimde nitelikli elektronik sertifika alma talebinde bulunabilme, kayıt otoritesi kavramının tanımlanabilmesi için hukuki bir zemin yaratma olarak özetlenebilir.

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 belirlemek,

Burada bahsedilen vekalet yetkisinin veya sertifika sahibinin sertifikada yer almasını istediği mesleki ve diğer kişisel bilgilerin de yukarıda bahsettiğimiz kimlik bilgilerinin tespiti yöntemiyle yapılması doğru bir yaklaşım olacaktır.

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,

İmza oluşturma verisi, iki şekilde üretilebilir. Veri hizmet sağlayıcı tarafından, sağlayıcıya ait araçlarla üretilir ve sertifika sahibine teslim edilir veya veri doğrudan sertifika sahibine ait araçla üretilir ve üretilen veri sağlayıcı tarafından tasdik edilir. Burada bahsedilen yükümlülükte, verinin sağlayıcı tarafından üretilmesi halinde sağlayıcı bu işlemin gizliliğini sağlamakla yükümlüdür, çünkü işlem sırasında veri başkaları tarafından kopyalanabilir. İkinci durumda veri, sağlayıcının sağladığı araçlarla üretilirse, bu işleyişin güvenliğini sağlamak yükümlülüğü hizmet sağlayıcıya aittir. Uygulamada sağlayıcı bu sorumluluğunu,

ancak kalitesi ispatlanmış güvenli araçları sertifika sahiplerine temin ederek veya bu araçların temini konusunda imza sahibini yönlendirerek yerine getirecektir.

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 bilgilendirmek,

Burada bahsedilen elektronik sertifika hizmet sağlayıcının imza sahibini aydınlatma yükümlüğünün bir gereğidir. Elektronik sertifika hizmet sağlayıcı bu aydınlatma yükümlülüğünü yukarıdaki kapsamda bir bilgilendirme yaparak yerine getirmek zorundadır. Elektronik sertifika hizmet sağlayıcı aydınlatma yükümlülüğü kapsamında yapacağı bilgilendirmeyi sertifikanın sertifikayı talep eden kişiye tesliminden önce yapacaktır. Buradaki teslim keyfiyetinin gerçekleşebilmesi için nitelikli elektronik sertifikanın zilyetliğinin sertifika talep eden kişi tarafından iktisap edilmesi gerekmektedir. Elektronik Sertifika Hizmet Sağlayıcısı bildirim yükümlülüğünü sertifika talep eden kişinin başvuruda bildirdiği elektronik posta adresine yapacağı güvenli elektronik imzası ile imzalanmış bir belgeyle yerine getirebilir.

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

Bu hükümde elektronik sertifika hizmet sağlayıcısın aydınlatma yükümlüğü kapsamındadır. Elektronik sertifika hizmet sağlayıcı imza oluşturma verisini başkasına kullandırmaması konusunda sertifika sahibini yukarıda belirtilen usulle bilgilendirdikten sonra bu konuyla ilgili sorumluluğunu yerine getirmiş olur. Bir başka deyişle sertifika sahibi kendi isteğiyle imza oluşturma verisini başkasına kullandırırsa ve bu durum sonucunda bir zarar meydana gelirse sağlayıcı bu zararı tazminle yükümlü olmaz.

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

Sertifika hizmet sağlayıcısının yaptığı hizmetlere ilişkin kayıtları saklama koşulları ve süreleri ile ilgili bir çok uluslararası standart bulunmaktadır. Karşılaştırmalı hukuktaki uygulamalarda da bahsi geçen standartlara atıfta bulunulduğundan kayıtları saklama süreleri bakımından yeknesaklık sağlanamamaktadır. Konuyla ilgili yönetmelik düzenlenirken süreler kadar, kayıt tutma koşulları da göz önüne alınmalı ve bunlarla ilgili şartlar da ortaya konulmalıdır. Kayıtları saklama süresinin belirlenmesinde bir diğer göz önünde bulundurulması gereken husus da sertifikaların kullanım süreleri geçtikten sonra da doğrulama yapabilmesine imkan verecek kayıtların tutulması ile mevzuatlarımızdaki zaman aşımı süreleri arasındaki uyumun sağlanmasıdır.

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

Burada bahsedilen bildirimin amacı, elektronik sertifika hizmet sağlayıcının hizmetleri sona erdikten sonra hizmetleri geçici olarak Kurumun veya başka bir sağlayıcının üstlenmesini sağlamak içindir. Yabancı uygulamada elektronik sertifika hizmet sağlayıcılarına hizmetlerini durduktan belli bir süre sonra dahi dizin (directory) ve iptal listesi (revocation list) hizmetlerini sunma zorunluluğu getirmektedir.

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

Burada bahsedilen işlem anahtar kurtarma (key recovery) işlemidir. Bu işlemde sertifika sahibi kapalı anahtarını (kanunun tabiri ile imza oluşturma verisini) kaybettiği takdirde veya başka özel durumlarda elektronik sertifika hizmet sağlayıcıda bulunan bir kopyasını kullanmaktadır. Özellikle Avrupa Birliği ülkelerinde kapalı anahtarın yedeklenme işlemi yasaklanmıştır. Ancak bizim kanunumdaki yasaklanma münhasıran elektronik sertifika hizmet sağlayıcıya yöneliktir. Elektronik sertifika hizmet sağlayıcı dışında üçüncü kişiler, imza sahibinin rızası olmak koşuluyla imza oluşturma verisinin kopyasını alabilir veya saklayabilir. Bu durum kendisini özellikle belli bir tüzel kişiliği temsilen kendisi adına sertifika düzenlenmiş gerçek kişiler de kendisini göstermektedir. Bu kişilerin bahsi geçen tüzel kişiliği temsilen imza oluşturma verisini kullandıklarından dolayı bu yetkinin

kendisinden alındıktan sonra daha önce bu kişinin yaptığı işlemlerde eğer sertifika sahibi imza doğrulama verisi ile aynı zamanda da şifreleme yaptı ise, şifrelenmiş olan tüzel kişiliğe ait olan kayıtlara bu tüzel kişiliğin ulaşması amaçlı olarak kullanılabilir. Ancak her halde imza oluşturma verisinin elektronik sertifika hizmet sağlayıcıları dışında üçüncü kişiler tarafından imza sahibinin rızası olmasına rağmen kopyasının alınmasında veya saklanmasında belli sınırlamaların olması gerekmektedir. Bu sınırlamaların kanunumuzda olmaması büyük bir eksikliktir. Zira kanunumuzda karşılaştırmalı hukuktaki örneklerin aksine imza sahibinin sorumluluğu düzenleyen hükümlere yer verilmemektedir.

5.2. Elektronik Sertifika Hizmet Sağlayıcısının Hukukî Sorumluluğu

Kanun'un 13. maddesinin 1. ve 2. fikralarına göre "*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*." Burada dikkat edilmesi gereken husus elektronik sertifika hizmet sağlayıcının sorumluluktan kurtulabilmesi için kusurunun bulunmadığını ispat etmesi gerekliliğidir. Maddede öncelikle açıklığa kavuşturulması gerekli olan durum üçüncü kişi kavramıdır. Karşılaştırmalı hukuktaki örnekler ve uygulamalar da incelendiğinde elektronik imza kullanımda taraf olan sujeler göz önünde bulundurularak sorumluluk rejimi belirlenmektedir. Yine karşılaştırmalı hukuk uygulamaları 3. kişi kavramını itimat eden tarafla (relying party) sınırlama eğilimi taşımaktadır. İtimat eden taraf kavramı elektronik imza kullanımda taraf olan ve elektronik imza ile imzalanmış belgelere veya bu elektronik imzanın ayrılmaz bir bileşeni olan elektronik sertifikada açıklanan bilgilere güvenerek işlemde bulunan kişidir. Bu tanımdan hareketle özellikle Elektronik Sertifika Hizmet Sağlayıcılarının sorumluluk kapsamını sadece itimat eden taraflarla sınırlı kılmak hem elektronik imzanın teknik ve hukuki kapsamı göz önünde bulundurulduğunda gerçekçi bir yaklaşım olacak hem de Elektronik Sertifika Hizmet Sağlayıcılarının hukuksal sorumluluk çerçevesini takibi, sonuçlanması ve karar verilmesi daha kolay bir çerçeveye çekmiş olacaktır. Elektronik sertifika hizmet sağlayıcının kusursuzluğunu ispat etme

yükümlüğü" getirilmesi, bir başka deyişle ispat külfetinin genel hükümlerin aksine yer değiştirilmesi ile "menfi durumun ispatı" gibi hukuken çok zor veya imkansız olan bir durumun ortaya çıkmasına neden olmuştur. Elektronik sertifika hizmet sağlayıcılarının elektronik imzanın kullanımında ve yaygınlaşmasındaki önemi göz önünde bulundurulduğunda bu kurumların sorumluluk rejimini genel hükümlere tabi tutmak hukuksal açıdan büyük bir yarar sağlayacaktır.

Kanunun 13. maddesinin 3. fıkrasında "*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*" denilmektedir. Burada elektronik sertifika hizmet sağlayıcıların, istihdam ettikleri personelin fiillerinden kusurları bulunmasa dahi sorumlu olacakları belirtilmiştir. Bu konu Borçlar Kanunu'nun 55. maddesinde belirtilen istihdam edenin sorumluluğu müessesesidir. Burada kusursuz sorumluluk mevcuttur, yani istihdam edenin zararı tazmin etmesi için kendi kusurunun bulunması zorunluluğu yoktur. Ancak BK 55. maddeye göre "böyle bir zararın vuku bulmaması için hal ve maslahatın icap ettiği bütün dikkat ve itinada bulunduğunu yahut dikkat ve itinada bulunmuş olsa bile zararın vukuuna mani olamayacağını ispat ederse mesul olmaz" şeklinde ifade edilen ve istihdam edene tanınmış olan bir kurtuluş beyinnesi imaknı vardır. Elektronik İmza Kanunu md. 13'e göre ise istihdam eden yani elektronik sertifika hizmet sağlayıcı bu kurtuluş beyyinesi ileri sürerek sorumluluktan ber'i tutulmaz. Madde bu haliyle ağırlaştırılmış kusursuz sorumluluk rejimini elektronik sertifika hizmet sağlayıcıları için öngörerek, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini çok daha fazla özen göstererek yürütmesini hedeflemekte, elektronik sertifika hizmet sağlayıcının yürüttüğü faaliyetlerin niteliğini göz önünde bulundurarak ortaya çıkacak tehlike sorumluğunun sosyal dengeleri göz önünde bulundurarak elektronik sertifika hizmet sağlayıcı üzerinde kalması amaçlamaktadır.

13. maddenin 4. fıkrasına göre; *"Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu*

ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir". Buna göre elektronik sertifika hizmet sağlayıcı ile sertifika sahibi arasında yapılacak, elektronik sertifika hizmet sağlayıcının sorumluluğunu ortadan kaldırmaya veya sınırlandırmaya yönelik anlaşmalar geçersiz olacaktır. Elektronik sertifika hizmet sağlayıcısının sertifika sahibine karşı sorumluluğunu sınırlandıran anlaşmaların içeriği ancak sertifikayla yapılacak işlemlerin niteliğine ve sertifikanın kullanıldığı işlemin mali değerine yönelik olabilecektir.

13. maddede belirtilen bir başka hukuki sorumluluk ise elektronik sertifika sağlayıcının sertifika mali sorumluluk sigortası yaptırma zorunluluğudur. Sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenecektir. Ancak burada Kanun'un kurgusuyla ilgili bir hata bulunmaktadır. Sigortaya ilişkin usul ve esasların yönetmelikle belirleneceği maddede belirtilmiştir fakat yönetmelikle belirlenecek hususların belirtildiği 20. madde de 13. maddeden bahsedilmemiştir. Bu usuli yanlışlık bir kenara bırakılırsa maddede belirtilen sertifika mali sorumluk sigortası neyin amaçlandığının açıklığa kavuşturulması gerekecektir. Maddede sigortanın kapsamı "elektronik sertifika hizmet sağlayıcısının Kanundan doğan yükümlüklerini yerine getirmemesi sonucu doğan zararlar"dır. Buradaki riziko "elektronik sertifika hizmet sağlayıcısının kanundan doğan yükümlülükleri yerine getirmemesidir". Elektronik sertifika hizmet sağlayıcılarının kanundan doğan yükümlülükleri sınırlı sayıda Kanun içersinde belirlenmiştir. Yine Kanuna göre sigorta ettiren elektronik sertifika hizmet sağlayıcıdır. Sigortalı veya sigorta lehdarı da elektronik sertifika hizmet sağlayıcıdır. Elektronik sertifika hizmet sağlayıcısının sertifikaları sigorta ettirerek sertifika kullanıcıları teslimi, sertifika kullanıcılarının sigorta lehdarı veya sigortalı olabilecekleri bir durum yaratsa da gerek kanunun gerekçesinde yapılan açıklamalar gerekse de kanunda tanımlanan riziko ve sigorta kapsamı göz önünde bulundurulduğunda sertifika kullanıcılarının sigortalı olması gibi bir durumun kanunkoyucu tarafından murad edilmediği ortaya çıkmaktadır. Karşılaştırmalı hukuktaki örnekler de incelendiğinde sertifika kullanıcılarının elektronik sertifika hizmet sağlayıcısı tarafından sigortalanması ihtiyari bir durumdur. Sigorta zorunluluğu sertifika hizmet sağlayıcılarının operasyonlarına bir başka deyişle kanundan doğan yükümlülüklerini yerine getirmemesine yönelik olarak kanunkoyucular tarafından düzenlemelere sevk edilmektedir.

6. Nitelikli Elektronik Sertifikaların İptal Edilmesi

Kanunun 11. maddesine göre; *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.

Burada belirilen koşullar karşılaştırmalı hukuktaki örnekler de incelendiği zaman bu örneklerle uyumluluk taşımaktadır. Avusturya'nın Elektronik İmzalarla İlgili Kanunu'nda yukarıda sayılan durumlara ek olarak sertifikanın kötüye kullanıldığının tespiti halinde de sertifika hizmet sağlayıcının sertifikayı iptal etmek zorunluluğu getirilmiştir.

Madde 11/2'ye göre *"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"* Burada bahsedilen sertifika iptal listesidir (Certificate Revocation List - CRL). Sertifika iptal listeleri; bir sertifika iptal edildiğinde bunun otomatik ve eşzamanlı olarak "sertifika kayıt veri tabanına" işlenmesi ve imzanın doğrulanması sırasında sertifikanın iptal edildiğinin belirlenebilmesi amacıyla kullanılırlar. Maddede belirtilen gereksinimler sertifika iptal işlemi için yeterli değildir, fakat madde 20'ye göre bu işlemin uygulanmasına ilişkin usul ve esaslar yönetmelikle belirlenecektir. Yönetmelikte sertifika iptal işlemi ile ilgili uluslararası standartlara atıf yapılması yararlı olacaktır.

11. maddenin son fıkrasına göre *"elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez"* Bu işleme retroaktif iptal yasağı denilmektedir. Karşılaştırmalı hukuktaki bir çok düzenlemede retroaktif iptal yasağına ilişkin

hükümler bulunmaktadır. Bu hükme göre elektronik sertifika hizmet sağlayıcıları iptal işlemini, işlemin yapıldığı günden önceki bir tarihten itibaren başlatamazlar.

Maddede belirtilen bir başka husus ise, elektronik sertifika hizmet sağlayıcının faaliyetine kurum tarafından son verildiğinde, elektronik sertifika hizmet sağlayıcısının elindeki sertifikaları başka bir elektronik sertifika hizmet sağlayıcıya teslim edilmesine Kurumun karar verecek olmasıdır. Sağlayıcı hizmetine kendisi son verirse bu durumda elindeki sertifikaları bir başka sağlayıcıya teslim etmelidir, eğer bunu durum gerçekleşmez ise elektronik sertifika hizmet sağlayıcı elindeki sertifikaları iptal etmekle yükümlüdür.

Kanunumuzda düzenlenmeyen ancak bir güvenlik tedbiri olarak yorumlanabilecek bir husus da sertifika hizmet sağlayıcının faaliyetlerine son verdiği durumda servis sağlayıcının sertifikasının akibetinin ne olacağı sorusu iptal prosedüründe önem kazanmaktadır. Konuyla ilgili Avusturya Elektronik İmza Kanunu'nun 9/5 maddesine göre; servis sağlayıcının hizmetleri yetkili kurum tarafından yasaklandığında yetkili kurum, servis sağlayıcının sertifikasını iptal etmektedir.

7. Kişisel Verilerin Korunması

Kanun'un 12. maddesine göre; *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

Maddedeki hükümler, Direktif ve yabancı mevzuatla uyumludur. Direktif'in 8. maddesi bilgilerin korunmasıyla ilgilidir ve kanunumuzda belirtilenlerle benzer yükümlülükler içermektedir. Ancak Direktif Md.8 ek olarak kişisel verilerin korunması ile ilgili 95/46/EC sayılı Direktif'e atıf yapmıştır. Karşılaştırmalı hukuktaki konuyla ilgili hükümlerde de kişisel verilerin korunması ile ilgili kanunlara atıflar bulunmaktadır. Ülkemizde de kişisel verilerin korunmasıyla ilgili bir kanun tasarısı mevcuttur. Tasarı kanunlaştığı takdirde karşılaştırmalı hukuktaki örneklerde olduğu gibi Yasanın 12. maddesine bu kanunla ilgili bir atıf hükmü sevk edilmelidir.

8. Yabancı Elektronik Sertifikalar

Kanunun 14. maddesine göre yabancı bir ülkede kurulu bulunan elektronik sertifika hizmet sağlayıcının sağladığı sertifikaların Türkiye'de Elektronik İmza Kanunu kapsamında hukuki değer tanınması iki yolla gerçekleştirilebilir. Bunlar; i) milletlerarası antlaşmalar veya ii) yabancı elektronik sertifikalara Türkiye'de mukim bir elektronik sertifika hizmet sağlayıcı tarafından garanti verilmesi durumlarıdır. Her iki durumda da yabancı elektronik sertifikalar Türkiye'de geçerli nitelikli elektronik sertifika ile aynı hukuki statüye sahip olacaklardır. Burada dikkat edilmesi gereken husus Türkiye'deki elektronik sertifika hizmet sağlayıcı tarafından garanti edilen yabancı sertifikaların kendi ülkelerinde nitelikli olup olmadıklarına bakılmaksızın, 5070 Sayılı Kanunda tanımlanan nitelikli elektronik sertifikalar ile aynı hukuki etki ve sonuçları sahip olacak olacaklarının kabul olunması durumudur. Garanti edilen sertifikanın kullanımı sonucu ortaya çıkabilecek zararlardan garanti eden sağlayıcı da sorumlu olacağı için; Yönetmeliklerle ortaya konulacak olan "garanti" etme yönteminin hem yurt içindeki elektronik sertifika hizmet sağlayıcıyı koruyucu niteliğe sahip olması hem de tüketicilerin haklarını gözetmesi gerekmektedir. Burada çapraz sertifikasyon (cross- certification) olarak bilinen yöntemin benimsenerek çapraz sertifkasyon yapacak olan elektronik sertifika hizmet sağlayıcıları arasındaki kural ve koşulların yönetmelik içersinde detaylandırılması doğru bir yaklaşım olacaktır.

9. Elektronik Sertifika Hizmet Sağlayıcılarının Denetimi

5070 Sayılı Kanun'a göre, elektronik sertifika hizmet sağlayıcıların faaliyetlerinin ve işlemlerinin denetimini yapmaya yetkili kurum Telekomünikasyon Kurumu'dur. Denetleme sırasında Kurumun yetkilendirdiği kişiler her türlü defter ve kayıtları inceleyebilir, sertifika sağlayıcının binalarına ve eklentilerine girebilir. Elektronik sertifika hizmet sağlayıcı bu durumlara kanunen rıza göstermek zorundadır.

Kanunumuzda denetlemeye ilişkin hükümler karşılaştırmalı hukuktakine göre çok daha belirsiz durumdadır. Direktif'in denetlemeyle ilgili 3.3 maddesine göre üye devletler kendi sınırları içerisinde nitelikli elektronik sertifika sağlayan hizmet sağlayıcıların denetimini yapmak üzere yetkili bir sistem kurmak zorundadır.

Avusturya[12]'da denetim kurumu i) sağlayıcının güvenlik ve sertifikasyon hükümleri ile ilgili belgesinde (security and certification policy) taahhüt ettiği hususları uygulamada yerine getirip getirmediğini ii) güvenli elektronik imzanın kullanımı halinde kanunda belirtilen gereksinimleri karşılayan araçların kullanılıp kullanılmadığını tetkik eder iii) hizmet sağlayıcıları kanunda belirtilen hükümler doğrultusunda akredite eder ve uygunluk denetimi yapan kurumların (confirmation body) işleyişini koordine eder. Ayrıca ülkede kurulu bulunan sağlayıcıların ve garanti edilen yabancı sağlayıcıların sertifikalarını denetim kurumu her zaman çevrimiçi olarak ulaşılabilecek bir dizinde tutar. Burada bahsedilen sağlayıcıların kendi sertifikalarıdır (CA certificate). Denetim kurumu kendi sertifikasını da yayınlamalı ve yukarıda bahsedilen dizini bu sertifika aracılığıyla imzalamalıdır. Denetim kurumunun sertifikası resmi gazetede yayınlanmaktadır.

Almanya[13]'da ise denetim kurumu, denetim işlemini özel kuruluşlar eliyle yapabilir. Kanunda denetim kurumunun sertifika hizmet sağlayıcının hizmetlerini yasaklayabileceği durumlar ile hizmet sağlayıcının elindeki sertifikaların iptalini emredebileceği durumlar ayrı ayrı sıralanmıştır.

---

[12] Avusturya Elektronik İmza Kanunu "SigG "md.13
[13] Almanya Elektronik İmza Kanunu "SigG "md.19

Avrupa Elektronik İmza Denetim Kurumları Forumu (FESA), Avrupa'daki konuyla ilgili denetim kurumları arasındaki işbirliğini sağlamak amacıyla kurulmuştur. Türkiye'yi temsilen Telekomünikasyon Kurumu FESA'ya üyedir. Kurumla ilgili FESA'nın web sitesinde yapılan açıklamada denetim ve ihtiyari akreditasyon konularında Kurumun yetkili olduğu gösterilmektedir. Oysa Kanunumuzda ihtiyari akreditasyon ile ilgili herhangi bir hüküm bulunmamakta ve bundan dolayı da Kurumun ihtiyari akreditasyon ile ilgili bir yetkisi ortaya çıkmamaktadır.

10. Ceza Hükümleri

Kanun'da ceza hükümleri, suçlar ve idari para cezaları olarak ikiye ayrılmıştır. Madde 16 ve 17'de imza oluşturma verilerinin izinsiz kullanımı ve sertifikalarda sahtekarlık fiiileri düzenlenmiştir.

Madde 16'ya göre güvenli elektronik imza oluşturma araçlarını ve verilerini sahibinden izinsiz olarak elde edenler, kullananlar, verileri kopyalayanlar ve araçları yeniden oluşturanlarla, izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar hapis ve para cezasıyla cezalandırılacaklardır. Bu hükümde açıklanması gereken nokta; "izinsiz elde edilen imza oluşturma aracı" bahsindeki iznin araç sahibinden mi yoksa Denetleme Kurumu veya benzer bir kurumdan mı alınacağı sorusudur. Eğer hükümde bahsedilen izin Kurum'dan alınacaksa, bu durumda imza oluşturma aracı elde etmek veya kullanmak için Kurum'dan izin alınması gerektiği gibi bir sonuç ortaya çıkacaktır. Oysa bu araçlar mevcut bilgisayar ağ sistemlerinde güvenli iletişim sağlanması için zaten kullanılmaktadırlar. Bu sebeple bunları elde etmek veya kullanmak için Kurum'dan izin alınması gerekliliği uygulamada kullanılamayacak bir hükümdür.

Madde 17'de ise sahte sertifikalar, geçerli sertifikaların tahribatı ve yetkisiz sertifika oluşturma ve bunları kullanma ile ilgili hükümler yer almaktadır. Burada problem yaratacak husus yetkisiz sertifika yaratma ve bunları kullanma ile ilgili olan hükümdür. Kanunda yetkisiz sertifika yaratma fiili ile ilgili bir açıklama bulunmamaktadır. Maddeden anlaşıldığı

üzere sertifika yaratmak için ayrıca yetkili olmak gerekmektedir, ancak kanunda sertifika yaratma ile ilgili yetkilendirilmeden bahsedilmemekle birlikte Direktif'in çok önem verdiği husus da sertifika hizmet sağlayıcıların herhangi bir izin veya yetkilendirme prosedürüne bağlı kalmadan faaliyetlerini yürütebilmesidir. Kanun'da yetkiyle ilgili bağdaştırılabilecek tek hüküm denetleme kurumuna yapılan hizmete başlama ile ilgili bildirimdir. Bu durumda maddeden çıkarılabilecek sonuç denetleme kurumuna bildirim yapmadan sertifika hizmeti sağlayan kişilerin yetkisiz kabul edileceğidir. Ancak daha öncede belirttiğimiz gibi elektronik sertifikalar sadece elektronik imza oluşturmak için kullanılmamakta bunun yanı sıra bilgisayar ağlarında güvenli iletişimin sağlanması için de kullanılmaktadır. Halihazırda kullanılmakta olan ağ iletişim sistemlerinin çoğunda sertifika ve açık anahtarlı altyapı kullanılmaktadır. Kanunun yetkisiz sertifika oluşturma ve bunları kullanmayla ilgili hükümlerine göre mevcut sistemlerde bu teknolojik altyapıyı kullanan operatörler, sistem kullanıcıları ve sistemi mülkiyetinde bulunduranlar Kanun'a göre suçlu durumunda olacaklardır. Bu sebeplerden dolayı yetkisiz sertifika oluşturanlar ve bunları kullananlar ile ilgili hüküm kanundan çıkartılmalıdır. İmza oluşturma verilerinin ve araçlarının izinsiz kullanımı ile sertifikalarda sahtekarlık ile ilgili suçları sertifika sağlayıcının personelinin işlemesi durumunda cezalar ağırlaştırılacaktır.

Kanun'un 18. maddesinde ise idari para cezalarına konu olan fiiller düzenlenmiştir. Kanun'da fiiller sıralanmamış fakat bunun yerine ihlali halinde para cezası verilecek hükümler sayılmıştır. Buna göre sertifika hizmet sağlayıcı; sertifika iptal hizmetini kanunda belirtildiği şekilde yapmadığı halde (md. 11), kanunla kendisine verilen yükümlülükleri yerine getirmediği halde (md.10), sigorta ile ilgili hükümleri ihlali halinde (md.13), denetimle ilgili hükümleri ihlali halinde (md. 15) idari para cezasına çarptırılacaktır.

Alman ve Avusturya kanunlarında konuyla ilgili hapis cezası öngören bir hüküm bulunmamaktadır. Ayrıca bu kanunlarda para cezasına tabi olacak fiiller aşağıdaki şekilde sıralanmıştır.

- Başkasının imza oluşturma verisini izinsiz kullanma
- Sertifika iptal ve dizin hizmeti sorumluluğunu yerine getirmeme

- Kanunda belirtilen kayıtları tutma sorumluluğunu yerine getrime
- Sertifika sahiplerine ve denetleme kurumuna gerekli bilgileri verme sorumluluğunu yerine getirmeme
- Güvenli elektronik imza oluşturma verisinin korunmasıyla ilgili gerekli önlemleri almama
- Güvenli elektronik imza araçlarını sertifika sahiplerine tavsiye etmeme
- Denetim kurumuna hizmet başlangıcı ihbarında bulunmama
- Sertifika sağlarken, sertifika talebinde bulunan kişilerden, kimliklerini kanıtlamayı sağlayacak yeterli kimlik bilgisinin alınmaması
- Sertifika sahibinden izinsiz olarak kanunda öngörülmeyen kişisel bilgilerin sertifikaya konması
- Hizmet sağlayıcının hizmetlerine son vermesi halinde durumdan denetim kurumun ve sertifika sahiplerini haberdar etmemesi ve elindeki sertifikaları başka bir sağlayıcıya devretmemesi

Avusturya ve Almanya uygulamasında yukarıda sayılan durumlarda sertifika hizmet sağlayıcıya idari para cezası verilir.

11. Kamu Kurum ve Kuruluşları Hakkında Uygulanmayacak Hükümler

Kanun'un Meclis Adalet Komisyonundaki görüşmelerinde yapılan bir değişiklikle Yasaya eklenen 21. madde ile "Elektronik Sertifika Hizmet Sağlayıcısı Faaliyetini" yerine getiren kamu kurum ve kuruluşları Telekomünikasyon Kurumunun denetiminden ve diğer elektronik sertifika hizmet sağlayıcılarının uymaları gerekli olan bir takım yükümlülüklerden muafiyet tanınmıştır. Bu durum özellikle Avrupa Birliği'nin Elektronik İmzalarla ilgili model alınmış olan Direktifine aykırılık teşkil etmektedir. Zira Direktifte ve Direktifin uygulanması ile ilgili yayınlanmış Komisyon belgelerinde Birliği Kuran Anlaşmanın 86. maddesi dayanak gösterilerek Elektronik Sertifika Hizmet Sağlayıcı olarak faaliyet gösteren kamu kurum ve kuruluşlarının rekabete aykırı davranmamaları ve monopol oluşturmamaları gerekliliği ifade edilmektedir. Kamu kurum ve kuruluşlarına bu konuda getirilecek istisnanın tarafsız, şeffaf,

ölçülü ve ayrımcılık yaratmayacak bir niteliğe sahip olması gerektiği ayrıca bu istisnanın ancak somut durumlar ve özel nitelikteki olaylar için belli bir kamu yararı ve zorunluluk bulunması koşuluyla tanınabileceği belirtilmektedir. Yasanın 21. maddesi ile kamu kurum ve kuruluşları lehine tanının bu istisna Birliğin yukarıda ortaya koyduğu prensiplere aykırılık teşkil etmektedir. Bu nedenle Yasanın 21. maddesi sadece yukarıda sayılan durumlarda ve ulusal güvenlikle ilgili işlemlerde bulunun sınırlı sayıda kamu kurum ve kuruluşları bakımından istisna tanınarak değiştirilmelidir. 21. Maddenin yaratacağı rekabete aykırı ortamın oluşumuna engellemek için Kurum gerekli tedbirleri almalı, özel sektör yatırımlarını dışlayıcı etki yaratacak olan kamu kurumlarının faaliyetlerini yakından takip ederek gerekli olan rekabet ortamının tesisi için azami çabayı göstermelidir.

12. İmza Sahibinin Yükümlülükleri

Kanunumuzda imza sahibinin yükümlülükleri düzenlenmemiştir. Oysa, Avusturya Elektronik İmza Kanunu'na göre[14] imza sahibinin imza oluşturma verisini koruma ve gerekli durumlarda sertifikayı iptal etme yükümlülüğü vardır. İmza sahibi imza oluşturma verisini elinden geldiğince saklı tutmalı ve izinsiz veriyi elde etme çabalarını engellemek için gerekli özeni göstermelidir. İmza sahibi eğer; imza oluşturma verisini kaybederse, imza oluşturma verisinin tehlikede olduğunu fark ederse veya sertifikadaki kişisel bilgiler değişmiş ise sertifika hizmet sağlayıcıya sertifikanın iptali ile ilgili talepte bulunmalıdır. Kanunumuzda imza sahibinin tanımı yapılmış fakat imza sahibinin yüklenmek zorunda olduğu sorumluluklar kanunda belirtilmemiştir. Elektronik imza kullanımının artması, sertifika sahiplerinin bilinçlendirilmesi ve sertifika hizmet sağlayıcıların güvenli bir ortamda hizmet sağlayabilmeleri için bu yükümlülüklerin kanunda sayılması gerekmektedir.

[14] SigG md. 21

İKİNCİ BÖLÜM – 5070 SAYILI KANUNUN UYGUNLANMASINA YÖNELİK OLARAK TELEKOMÜNİKASYON KURUMUNUN YÖNETMELİKLE DÜZENLEME YAPACAĞI ALANLAR VE YÖNETMELİKTE GÖZ ÖNÜNDE BULUNDURULMASI GEREKEN TEMEL İLKELER

1. Genel Hükümler

"Genel Hükümler" bölümünde Yönetmeliğin amaç, kapsam, hukuki dayanak, tanımlar ve ilkeler bölümleri bulunmalıdır. Hukuki dayanak kısmı Kanunun Yönetmelikle düzenlenecek konularının belirlendiği 20. maddesine dayanılarak hazırlanmalıdır. Buna göre Yönetmelik, Kanunun 6, 7, 8, 10, 11 ve 14. maddelerinde belirtilen konuların uygulanmasına ilişkin usul ve esasların ortaya konması amacıyla hazırlanmalı ve Yönetmeliğin kapsamı bu maddelerdeki konularla sınırlı olmalıdır.

Yönetmeliğin *"Tanımlar"* bölümünde, Kanunda tanımları yapılmayan fakat Yönetmelikle düzenlenen konuların daha iyi açığa kavuşturulabilmesi için, tarif edilmesi zorunlu olan hususların tanımları yapılmalıdır. Bu bölümde alt sertifika otoritesi, kayıt otoritesi, bildirimi inceleyecek kurul, zaman damgası hizmet sağlayıcısı, dizin ve sertifika iptal listesi hizmet sağlayıcısı, sertifika iptal listesi, faaliyet raporu gibi konuların tanımları yapılmalıdır. Özellikle alt sertifika otoritesi ve kayıt otoritesinin tanımlarının yapılması, bu yapıların Kanun kapsamında sertifika hizmet sağlayıcısı olmadıklarının hukuki olarak açıklığa kavuşması için gereklidir. Avrupa da çoğu düzenlemede bu tanımların yapılmamış olması uygulamada sertifika hizmet sağlayıcılara, düzenleyici kurumlara ve mahkemelere zorluklar çıkarmaktadır.

Genel hükümler bölümünde en son olarak Yönetmeliğin yorumlanmasında gözetilecek *"Temel İlkeler"* ortaya konmalıdır. Bu temel ilkelerin ortaya konması ile Yönetmeliğin yorumlanması bakımından kolaylık sağlanacaktır. Sözkonusu temel ilkeler serbest rekabet ortamının oluşturulması, tüketici haklarının korunması, ülkede elektronik sertifika ve elektronik imza kullanımının yaygınlaştırılmasıdır.

2. Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

Kanunun 6. ve 7. maddelerinde tanımları ve nitelikleri belirtilen güvenli elektronik imza oluşturma ve doğrulama araçları, Yönetmelikle ayrıntılı olarak olarak düzenlenecektir. Araçlar hakkında Yönetmelikle düzenlenmesi gereken konular; güvenli elektronik imza oluşturma araçlarının ürün bazında tanımlanması ve kamuoyuna duyurulması, araç sahiplerinin sorumlulukları, araçlarda kullanılacak güvenlik arayüzleri ve şifreler (PIN), sertifika hizmet sağlayıcıların kullanacağı teknik araçlar, güvenli elektronik imza oluşturma ve doğrulama araçlarına ilişkin uluslararası standartlardır.

- *Kurumun güvenli elektronik imza oluşturma araçlarını tanımlaması*

5070 sayılı Kanuna göre elle atılmış imza (ıslak imza) ile aynı hukuki değere sahip tek elektronik imza güvenli elektronik imzadır. Güvenli elektronik imza oluşturabilmek için, imza sahibinin sertifikasının nitelikli olması ve imzalamak için kullandığı aracın güvenli elektronik imza oluşturma aracı olması gerekmektedir. Kullanıcı açısından bakıldığında, hangi sertifikanın nitelikli ve hangi aracın güvenli olduğunun açıkça anlaşılabilmesi gerekmektedir. Kanunun 9. maddesinde belirtildiği üzere nitelikli elektronik sertifikalarda *"nitelikli elektronik sertifika"* ibaresinin bulunması zorunludur. Güvenli elektronik imza oluşturma araçları ile ilgili olarak böyle bir zorunluluk bulunmamaktadır. Bu sebepten ötürü, kullanıcıların elektronik imza kullanımından kaynaklanabilecek mağduriyetini engellemek ve elektronik imza kullanımını kullanıcılar açısından daha güvenli hale getirebilmek için, ürün bazında hangi araçların güvenli elektronik imza aracı olduklarının tespiti ve bunu kamuoyuna duyurulması gerekmektedir.

Güvenli elektronik imza oluşturma araçlarının akreditasyonuyla ilgili olarak iki sistem önerilebilir. Bunlardan ilki; ülke içinde bir kurumun, araçların Kanun ve Yönetmelikle belirlenen gereksinimlere ve uluslararası standartlara uygunluğunu denetlemesidir. Bu sistemde yetkili kurum araçların teknik uyumluluk testlerini kendisi yapmaktadır. İkinci sistemde ise; aynı denetim yurtdışında yerleşik bir kurum tarafından yapılmakta ve bu

kurumun araca verdiği güvenilirlik belgesi, yurtiçindeki bir kurum tarafından onaylanmaktadır. İlk sistemle ilgili olarak Avrupa Komisyonu'nun uyumluluk kurumlarının (confirmation body) kriterlerini belirlediği bir kararı bulunmaktadır (2000/709/EC). Türkiye'de böyle bir kurumun kurulması veya Telekomünikasyon Kurumu'nun kendi bünyesinde elektronik imza araçlarıyla ilgili bir akraditasyon bölümü oluşturması halinde Komisyon'un kararı dikkate alınmalıdır. Akreditasyon işleminin teknik testlerini yapabilecek bir kurumun bulunmaması durumunda ise ikinci yöntem benimsenebilecektir.

Güvenli elektronik imza araçlarının Kurum tarafından kayıt altına alınması ve kamuoyuna duyurulmasının prosedürü Kurum tarafından çıkarılacak Yönetmelikte ve konuyla ilgili hazırlanacak matbu belgelerde belirtilmelidir. Yukarıda da belirtildiği üzere kullanıcı güvenliğinin sağlanması için güvenli elektronik imza oluşturma ve doğrulama araçlarının Kuruma kaydettirilmesi zorunluluk haline getirilmelidir. Piyasaya güvenli elektronik imza sürmek isteyen satıcılar ürünlerini; yurtdışından aldıkları, ürünlerin Yönetmelikle belirtilen uluslararası standartlara uygun olduğunu tasdikleyen belgeleriyle birlikte Kurumun hazırladığı matbu belgeleri doldurarak, Kuruma kayıt ettirmelidir. Kurum güvenli imza oluşturma aracı olarak kayıt altına aldığı bu ürünleri, web sitesinden duyurmalıdır. Güvenli elektronik imza oluşturma araçlarının ilanı için tebliğ, genelge, resmi gazete ilanı gibi yolların kullanılması tavsiye edilir.

- *Elektronik imza oluşturma aracı sahibinin sorumluluğu*

Güvenli elektronik imza oluşturma araçları, teknik olarak imza oluşturma verilerini içlerinde barındırdıkları için bu araçların da korunması ve hırsızlığa karşı özenle saklanması gerekmektedir. Bu sorumluluk, araçlar araç sahibinde bulunduğu için onlara yüklenmelidir.

Bilindiği üzere güvenli elektronik imza oluşturma araçları hem yazılım hem de donanım şeklinde olabilmektedir; araç sahibinin aracı koruma yükümlülüğü açısından yazılım ve donanım için farklı yükümlülükler getirilebilir. Buna göre yazılım bazlı araçların korunmasında, araç sahibinin hem yazılımını koruması hem kapalı anahtarın bulunduğu dizini koruması hem de yazılımın çalıştığı terminalini (bilgisayar, palm, cep telefonu) koruması gerekmektedir. Bu koruma hem fiziksel koruma hem de hem diğer yazılımlara karşı koruma

olarak ikiye ayrılabilir. Fiziksel korumada araç sahibi yazılımın çalıştığı ve kapalı anahtarın bulunduğu terminalini dışarıdan gelecek müdahalelere karşı korumalıdır. Bu kapsamda terminale ek bir araç takılarak veya basit bir fiziksel müdahale ile kapalı anahtarın çalınması veya elektronik imza oluşturma aracının çalıştırılması kullanıcı tarafından engellenmelidir. Kullanıcı bu tür müdahalelere karşı yeterli güvenlik seviyesine sahip terminaller kullanmalıdır. Diğer yazılımlara karşı korumadan kastedilen ise; imza oluşturma aracının ve bulunduğu terminalin zararlı yazılımlara (bilgisayar virüsleri, trojan, worm) karşı korunmasıdır. İmza aracı sahibi bu korumayı sağlamak için en azından güvenlik programları (antivirüs programları, firewall) kullanmalıdır.

Güvenli elektronik imza oluşturma aracının donanım bazında olması halinde, araç sahibinin aracın çalınmasını engellemek için gereken özeni gösterme sorumluluğu bulunmaktadır. Ayrıca yetkisiz elektronik imza kullanımını engellemek amacıyla araç sahibi, aracını başkalarına kullandırmamalıdır.

Araç sahibinin imza oluşturma araçlarını koruma, saklama ve güvenliği için gerekli özeni gösterme sorumluluğu dışında; "imza oluşturma verisini" de ayrıca koruma, saklama, başkalarına kullandırmama ve çalınmasını engellemek için gerekli özeni gösterme sorumluluğu bulunmaktadır. Bu iki süje için birbirinden ayrı olarak sorumlulukların tanımlanması, süjelerin birbirinden ayrı olarak kullanılabilmesi ve erişilmesi sebebiyle gereklidir.

Güvenli elektronik imza oluşturma ve doğrulama araçlarının güvenli olarak sayılabilmesi için bu araçların, araç sahibi adına kayıtlı olması gerekmektedir. Bu ancak lisanslı yazılım kullanılması ile mümkün olabilecektir. Böylece yazılım bazlı elektronik imza oluşturma aracı sadece tek kişi tarafından (lisans sahibi) kullanılabilecek ve aracın kullanıcı tarafındaki güvenlik seviyesi arttırılacaktır. Ayrıca böyle bir düzenlemeyle korsan yazılım kullanımının önüne geçilecektir. Bu sebeplerden ötürü Yönetmelikle açıkça yazılım bazlı güvenli elektronik imza oluşturma araçlarının lisanslı olması zorunluluğu getirilmelidir.

- *PIN*

Yazılım bazlı güvenli elektronik imza oluşturma araçlarının, kullanıcı tarafındaki güvenliklerinin arttırılması için, bazı bilgi güvenliği araçlarına ihtiyaç duyulmaktadır. Bunlar biometrik uygulamalar ve PIN şeklinde olabilir. Piyasada biometrik uygulamalarla çalışan araçların sayısının az olması ve fiyatlarının çok pahalı olması sebebiyle, biometrik güvenlik zorunluluk olarak düzenlenmemelidir. PIN uygulamaları ise yabancı mevzuatta da düzenlendiği üzere, elektronik imza araçlarının güvenliklerini arttırmak için zorunluluk olarak düzenlenebilir. Yazılım bazlı güvenli elektronik imza oluşturma araçlarının aktive edilmesi, aktivasyon öncesi PIN kullanımı gerektiren bir arayüz taşımasına bağlı olmalıdır. Böylece sadece PIN'i bilen araç sahibi, aracı aktif hale getirebilecektir. Ancak burada dikkat edilmesi gereken bazı hususlar bulunmaktadır: Bir imza oluşturma aracı, imza oluşturma fonksiyonu dışında başka fonksiyonlar için de kullanılabilir. Bu şekilde çok fonksiyonlu bir imza oluşturma aracında, PIN imza oluşturma fonksiyonuna ait olmalı veya imza oluşturma fonksiyonu için ayrı PIN tanımlanmalıdır. Araç sahibinin ayrıca bu PIN'i de saklama, koruma ve başkalarına söylememe yükümlülüğü vardır. Dikkat edilmesi gereken bir başka husus ise; imza oluşturma araçlarının güvenliğini arttırmak için kullanılan bilgi güvenliği araçlarının, aracın kullanılabilirliğini azaltmamasıdır; zira birçok PIN kullanımı, aracın kullanılabilirliğini azaltacaktır. Sonuç olarak yazılım bazlı imza oluşturma araçlarında PIN kullanımı Yönetmelikle zorunlu hale getirilmeli ancak öngörülen sistemle aracın kullanılabilirliği azaltılmamalıdır.

- *Sertifika hizmet sağlayıcıların kullanacağı teknik araçlar*

Sertifika hizmet sağlayıcılarının son kullanıcı ve alt sertifika otoritesi sertifikalarını yaratmak ve imzalamak için kullandıkları araçların sahip olması gereken minimum gereksinimler yönetmelikle ortaya konulmalıdır. Elektronik sertifikalarda güvenlik, sertifika zincirindeki ilk elemandan son elemana kadar önem taşımaktadır. Bir sertifikanın nitelikli sertifika olabilmesi için, hiyerarşik sertifika zincirinde kendisinden önce gelen Alt sertifika otoritesi sertifikalarının ve kök sertifikanın da nitelikli sertifikanın yerine getirmesi gereken minimum gereksinimlere sahip olması gerekmektedir. Bu sistemin oluşabilmesi için, sertifika hizmet sağlayıcıların kullanacağı teknik araçların gerekli güvenlik seviyesine sahip olmaları

gerekmektedir. Avrupa Komisyonu'nun 2003/511/EC sayılı kararında, sertifika hizmet sağlayıcıların kullanması gereken araçlarla ilgili CEN standartları referans gösterilmiştir. Karara göre bu standartları yerine getiren araçlar Komisyon'un Elektronik İmza Direktif'inde belirtilen koşulları (Ek.2/f) yerine getirmiş sayılacaklardır. Elektronik imza kullanımında karşılıklı işlerliğin sağlanması ve ülkede oluşturulacak sistemin Avrupa Birliği'nde kullanılan sistemle uyumlu olması amacıyla Yönetmelik'te Komisyon'un referans gösterdiği standartların kullanılması uygun olacaktır. Komisyon kararında CEN'in CWA 14167-1 ve 14167-2 numaralı standartlarını referans göstermiştir. Bu referanslara ek olarak CEN 14167-3 numaralı standardı da yayınlamıştır.

- *Güvenli elektronik imza oluşturma ve doğrulama araçlarına ilişkin standartlar*

5070 sayılı Kanun'un 6. ve 7. maddelerinde imza oluşturma ve doğrulama araçlarıyla ilgili kriterler belirtilmiştir. Burada sayılan kriterler teknoloji-bağımsız bir dille yazılmış oldukları için aracın güvenlik seviyesinin belirlenmesinden çok tanımının yapılmasına yaramaktadırlar. Bilindiği üzere elektronik imzada kullanılan kriptografi sistemi teknik bir sistemdir ve bu sistemi kullanan güvenli bir aracın tanımının teknik metinlerle yapılması gerekmektedir. Elektronik İmza Direktifi'nin EK - 3 kısmında güvenli elektronik imza oluşturma ve araçlarının kriterleri belirtilmiştir. Ayrıca Komisyon 2003/511/EC sayılı kararıyla güvenli elektronik imza oluşturma araçlarıyla ilgili CEN'in yayınladığı 14169 numaralı standardı referans göstermiştir. Yönetmelikte de bu standart güvenli elektronik imza oluşturma araçlarıyla ilgili olarak referans gösterilmelidir. Güvenli elektronik imza doğrulama araçlarıyla ilgili olarak uluslararası bir standart belirlenmemiştir. Bu sebeple Yönetmelikte de doğrulama araçlarıyla ilgili olarak bir standardın şimdilik referans gösterilmemesi gerekmektedir. Ancak elektronik imza oluşturma araçları, aynı zamanda doğrulama aracı olarak da kullanılabildikleri ve oluşturma araçları için, öngörülen teknik gereksinimlerin doğrulama araçları için de geçerli olması sebebiyle, doğrulama araçları için de oluşturma araçları için öngörülen standartlar kullanılabilir.

3. **Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri**

- *SHS'nin asgari hizmetleri*

Yönetmelikte sertifika hizmet sağlayıcının sağlaması gereken asgari hizmetler belirlenmelidir. Bu nitelikler ayrıca Kurum tarafından hazırlanacak, matbu bildirim formunda da bulunabilir. Asgari hizmetler arasında;

1. Kendi kök sertifikası altında nitelikli elektronik sertifika yayınlama

Kanun kapsamında bir elektronik sertifika hizmet sağlayıcısının, kendi kök sertifikasını yayınlaması ve son kullanıcı sertifikalarını bu kök sertifika altında yayınlaması gerekmektedir.

2. 7/24 teknik destek (web sayfası, çağrı merkezi)

Sertifika hizmet sağlayıcı sertifika ve imza kullanımıyla ilgili olarak sertifika sahiplerini teknik ve hukuki açıdan bilgilendireceği, sertifika iptal taleplerini alabileceği 7/24 çalışan bir web sayfası ve çağrı merkezi kurmalıdır.

3. Sertifika politikası ve sertifika uygulama hükümleri belgelerinin hazırlanması ve yayınlanması

Sertifika hizmet sağlayıcı, kendi altalanı içinde sertifika kullanımıyla ilgili kuralları belirlemek amacıyla, yukarıda bahsedilen belgeleri hazırlamalıdır. Sertifika hizmet sağlayıcının başka bir sertifika hizmet sağlayıcıyla çapraz sertifikasyon yapması durumunda bu belgeleri diğer sertifika hizmet sağlayıcının belgeleriyle uyumlu hale getirmesi gerekmektedir.

4. Anahtar ve sertifika yaşam döngüsü kontrolleri

Sertifika hizmet sağlayıcı; anahtar üretimi, saklanması, yedeklenmesi, kurtarılması, dağıtılması, yok edilmesi gibi konularda hizmetlerinin ne şekilde olduğunu yapacağı bildirimle ortaya koymalı ve hizmetlerinin uluslararası standartlara uygunluğunu kanıtlamalıdır.

5. Personelin nitelikleri

Sertifika hizmet sağlayıcı sertifika hizmetlerinin yürütümünü üstlenebilecek ve Yönetmelikle belirlenen niteliklere sahip personel çalıştırmalıdır. Ayrıca sertifika hizmet sağlayıcı, sertifika hizmetleri ve özellikle alt sertifika otoritelerinin kapalı anahtarlarının oluşturulmasıyla (seremoni) ilgili olarak personel yetki çizelgesini hazırlamalıdır.

6. Operasyon merkezinin fiziksel ve çevre güvenliği

Sertifikaların ve imza oluşturma verilerinin üretimi için, sertifika hizmet sağlayıcı uluslararası standartlara uygun bir sertifika operasyon merkezi kurmalıdır. Bu merkez dışarıdan gelebilecek tehlikelere ve müdahalelere karşı yeterli güvenlik altyapısına sahip olmalıdır.

7. Sistem izleme ve denetleme

Sertifika hizmet sağlayıcı hizmetlerinin yürütümü ve sisteminin işlemesiyle ilgili iç denetimlerini yapmalı ve bu denetimlerle ilgili kayıtlarını tutmalıdır.

- *Bildirim*

Elektronik sertifika hizmet sağlayıcısı, Kanunun 8. maddesi uyarınca faaliyete başladığına ilişkin Kuruma bildirim yapacaktır. Bildirimde sertifika hizmet sağlayıcı, faaliyetlerinin hukuki ve teknik yönleriyle ilgili olarak Kuruma bilgi verecektir. Kurum, sertifika hizmet sağlayıcının bildirimle ortaya koyduğu faaliyetlerinin Kanuna ve Yönetmeliğe uygunluğunu denetleyecek ayrıca bildirimde belirtilen hususların sertifika hizmet sağlayıcı tarafından yerine getirilip getirilmediğini kontrol edecektir.

Bildirim ve bildirimin denetlenmesi işlemlerinin kolaylaştırılması için bildirimin formatının ve içeriğinde bulunması gereken bilgilerin önceden belirlenmesi faydalı olacaktır. Bu sebeple bildirim formunun, matbu form şeklinde Kurum tarafından hazırlanması gerekmektedir. Sertifika hizmet sağlayıcılar Kurumun web sitesinden temin edecekleri bu matbu form ile Kuruma bildirimde bulunabileceklerdir.

Bildirimde, sertifika hizmet sağlayıcının yerine getirmesi gereken şartlar Webtrust veya ETSI'nin konuyla ilgili standartlarından yol çıkarılarak hazırlanmalıdır. Bu doğrultuda bildirimde, sertifika hizmetleriyle ilgili hukuki ve teknik konular ele alınmalıdır. Bildirimle sertifika hizmet sağlayıcı; kullanacağı teknik araçların güvenliği, yayınlacağı sertifikaların nitelikleri, personelin nitelikleri, sertifikaların üretileceği operasyon merkezinin fiziki güvenliği, sertifika talebinde bulunulan kimselere verilen bilgilendirme hizmeti, imzalama işlemiyle ilgili olarak kullanıcılara verilen teknik ve hukuki bilgilendirme desteği gibi konularda açıklamalar yapacaktır. Ayrıca bildirimde bulunan sertifika hizmet sağlayıcının yerine getirmesi gereken tüketicinin korunması ile ilgili şartlar açısından; sertifika hizmet sağlayıcıdan, son kullanıcılarla yapacağı sözleşmeler Kurum tarafından incelenmek üzere istenebilir.

Elektronik sertifika hizmet sağlayıcıların Kuruma yapacakları bildirimin, Kuruma bildirilme usulü de Yönetmelikle belirlenmelidir. Güvenliğin sağlanması amacıyla bildirimin sadece elden teslim yoluyla yapılması uygun olacaktır. Posta veya elektronik ortamda bildirim yollanmasına izin verilmemelidir.

Bildirimde belirtilecek hususların elektronik sertifikalar ve elektronik imzalar konusunda spesifik bilgi gerektirmesi sebebiyle, bildirimi inceleyecek kişilerin konuyla ilgili yeterli donanıma sahip olmaları gerekmektedir. Bu sebepten dolayı Kurum kendi içinde bildirim inceleme ve sertifika hizmet sağlayıcıları denetleme konusunda yetkili bir Kurul tanımlamalıdır. *"Bildirim İnceleme Kurulu"* veya *"Denetleme Kurulu"*'nun görev ve yetkileri Yönetmelikle belirlenmelidir. Ancak burada dikkat edilmesi gereken husus Kurulun görevleri ve yetkileri tanımlanırken, bu hususun hukuki dayanağının Kanunun 8. maddesi olduğudur. Kurul inceleme ve denetleme yetkisini, Kanunun 8. maddesinde belirtilen bildirimi inceleme ve sertifika hizmet sağlayıcıının faaliyetlerinin bildirime uygunluğunu denetleme konularına dayanarak elde etmektedir. Kurumun Kanunun 15. maddesine dayanarak denetleme yetkisi de bulunmaktadır. Ancak 15. madde Yönetmelikle düzenlenecek maddelerden olmadığı için denetleme hususunda Yönetmelikle düzenleme yapmak mümkün değildir. Kurum Kanundan kaynaklanan denetleme yetkisini, bildirim inceleme görevini yerine getirirken de kullanabilecektir. Bu doğrultuda Kurum sertifika hizmet sağlayıcılarının faaliyetlerinin bildirime uygunluğunu denetlerken *"sertifika hizmet sağlayıcının her türlü defter, belge ve*

kayıtlarını inceleyebilir, yönetim yerleri, binalar ve eklentilere girebilir, çalışanlardan yazılı ve sözlü bilgi alabilir". Sonuç olarak Kurum denetleme yetkisini konuyla ilgili spesifik bilgiye sahip personelinden oluşan ve Yönetmelikte nitelikleri, görevleri ve yetkileri tanımlanan "Kurul" aracılığıyla yapacaktır. Kurul ilk önce, sertifika hizmet sağlayıcının faaliyetlerinin Kanuna ve Yönetmeliğe uygunluğunu, sertifika hizmet sağlayıcının yapacağı bildirimle inceleyecek; bildirimin uygun bulunması durumunda, sertifika hizmet sağlayıcının faaliyetlerinin bildirime uygunluğunu denetleyecektir.

- *Kurumun sertifika hizmet sağlayıcılardan talep edeceği ücretler*

Kurumun elektronik sertifika pazarını regüle etmesi, pazardaki oyuncuları denetlemesi, sertifika hizmet sağlayıcıların yapacakları bildirimleri incelemesi ve kamuoyunu elektronik imza kullanımı konusunda bilgilendirmesi için mali kaynağa ihtiyacı olacaktır. Bu mali kaynak piyasadaki sertifika hizmet sağlayıcılardan ve güvenli elektronik imza oluşturma ve doğrulama aracı satıcılarından temin edilmelidir.

Kurumun talep edeceği ücretlerin belirlenmesinde şu ilkeler gözönünde bulundurulmalıdır;

1. Talep edilecek ücretler sertifika hizmet sağlayıcıların piyasaya girmelerini engelleyecek boyutlarda olmamalıdır,
2. Sertifika hizmet sağlayıcıları Kuruma ödeyecekleri ücretleri, sertifika fiyatlarına yansıtacakları için, ücretler kullanıcıların sertifika almalarını engelleyecek boyutlarda olmamalıdır,

Kurumun hangi işlemler için ücret talep edeceği noktası da, Yönetmelikle belirlenmesi gereken hususlardan biridir. Kurum sertifika hizmet sağlayıcılardan, faaliyete başlama bildiriminin incelenmesi ve sertifika hizmet sağlayıcılarının faaliyetlerinin denetlenmesi işlemleri için ücret talep edebilir. Güvenli elektronik imza oluşturma ve doğrulama araçları satıcılarından ise, ürünlerin Kurum tarafından tasdik edilmesi ve kamuoyuna duyurulması işlemleri için ücret talep edebilir.

- *Faaliyete son verme, faaliyeti durdurma*

Kurum, 8. madde dolayısıyla, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini, bildirimde yer alan şartları yerine getirmemeleri sonucunda durdururabilir ve Kanunda belirtilen sürenin sonunda faaliyete son verebilir. Bu süreç, sertifika hizmet sağlayıcının faaliyetlerinin devamı sırasında, bildirimde belirtilen şartları kaybetmeleri sonucunda da uygulanır.

Kurum, sertifika hizmet sağlayıcıların faaliyetlerinin devamı sırasında Kanunda, Yönetmelikte ve bildirimde belirtilen şartların yerine getirilip getirilmediğini, sertifika hizmet sağlayıcılara yapacağı denetimlerle ve sertifika hizmet sağlayıcılardan periyodik olarak alacağı *"faaliyet raporlarıyla"* belirlemelidir. Faaliyet raporlarında sertifika hizmet sağlayıcıları, bildirimde belirttikleri hizmetlerin yürütümü ve kullandıkları araçların teknik özellikleri konusunda bilgi vermelidirler. Faaliyet raporlarının incelenmesi görevi de *"bildirim inceleme kurulu"* tarafından yerine getirilebilir.

Sertifika hizmet sağlayıcının faaliyetlerine son verilmesi veya faaliyetlernin durdurulması sonucunda, sertifika hizmet sağlayıcının yayınlamış olduğu sertifikaların ve sertifika iptal listelerinin ne şekilde ve hangi sertifika hizmet sağlayıcısına devredilmesi gerektiği konusu, Yönetmelik Şablonu'nun Dördüncü Bölümünde yer alan *"Dizin ve İptal Hizmetlerinin Devri"* kısmında açıklandığı üzere çözüme kavuşturulmalıdır. Bu sebepten dolayı ilgili maddeye atıf yapılarak sorun çözülebilir.

- *Sertifika ücretleri alt ve üst sınırları*

Kanunun 8. maddesine göre; elektronik sertifika hizmet sağlayıcıları, Kurumun elektronik sertifikaların ücretleriyle ilgili belirleyeceği alt ve üst sınırlara uymak zorundadır. Kurum sertifika ücretlerinin alt ve üst sınırlarını belirlerken, sertifika piyasasının oluşumuna zarar vermemeli, sertifika hizmet sağlayıcıların faaliyetlerini sürdürmelerini engelleyecek fiyatlar öngörmemelidir. Belirlenecek fiyatlar ile elektronik sertifika kullanımının özendirilmesi hedeflenmelidir.

Kurum, ücret skalasını ortaya koyarken, sertifikaların maliyetlerini gözönünde bulundurmalı ve maliyet bazlı hesaplama yöntemiyle ücretleri tespit etmelidir. Ancak sertifika maliyetlerinin belirlenmesinde; sertifikanın maliyetiyle üretilen sertifika arasında ters orantı olduğu unutulmamalıdır. Bu sebepten dolayı, ücret alt ve üst sınırları arasında geniş bir ölçek bulunmalıdır, zira piyasadaki sertifika hizmet sağlayıcılarının üretecekleri sertifika sayısı biribirinden farklılık arzedecektir.

- *Sertifika hizmet sağlayıcının personelinin sahip olması gereken nitelikler*

Sertifika hizmet sağlayıcının personelinin bazı teknik bilgilere sahip olması, elektronik sertifika işlemlerinin yürütülmesi için zorunludur. Bilindiği üzere elektronik sertifika ve elektronik imza hizmetleri kriptografi, açık anahtarlı altyapı, bilgi güvenliği gibi konularda yüksek teknoloji bilgisi gerektirmektedir. Ayrıca elektronik imzanın hukuki değeri yüzünden, elektronik imzanın bileşenleri ve elektronik sertifika hizmet sağlayıcılarıyla ilgili olarak hukuki düzenlemelerde uluslararası standartlara atıf yapılmaktadır. Dolayısıyla sertifika hizmet sağlayıcıların çalıştıracakları teknik personelin, uluslararası standartlar konusunda da yeterli bilgiye sahip olmaları gerekmektedir.

Sertifika hizmet sağlayıcıların, çalıştıracakları personelin teknik bilgisini, Kuruma kanıtlamaları gerekmektedir. Kurum sertifika hizmet sağlayıcılarını denetlerken, personelin kalifikasyonunu da objektif kriterler doğrultusunda değerlendirmelidir. Bu nedenle personelin teknik bilgisi lisans, yüksek lisans, sertifika gibi belgelerle kanıtlanmalıdır.

Sertifika hizmet sağlayıcının, sadece teknik personelinin niteliklerinin Yönetmelikle belirlenmesi uygun olacaktır. Çünkü teknik hizmetler dışında elektronik sertifika hizmet sağlayıcı en azından müşteri desteği, pazarlama, halkla ilişkiler ve hukuk alanlarında da personel çalıştırmak durumunda kalacaktır. Bu sebeple Yönetmelikte sadece teknik personelin nitelikleri zorunlu olarak belirtilmelidir.

Yönetmelik Şablonunda teknik personelin nitelikleri belirlenirken sadece olumlu özelliklere yer verilmiştir. Olumsuz özelliklere (yüz kızartıcı suç işlememe, hürriyeti bağlayıcı suç işlememe) yer verilmemesinin sebebi, bu özelliklerin neler olduğunun

listelenmesi ve değerlendirilmesi hususunun sertifika hizmet sağlayıcıların inisiyatifine bırakılmasıdır. Ancak zaten Kanuna göre; sertifika hizmet sağlayıcıları çalıştırdıkları personelin konuyla ilgili fiillerinden dolayı sorumlu oldukları ve bununla ilgili kurtuluş beyyinesi ileri süremedikleri için, olumsuz niteliklere sahip bir kişiyi çalıştırma konusunda çok da serbest olacakları söylenemeyecektir.

- *Sertifika kayıtları ve kimlik tespiti*

Uygulamada sertifika kayıtları sırasında kimlik tespiti iki yöntemle yapılabilir;

✓ Doğrudan tespit yöntemi

Sertifika hizmet sağlayıcı talep sahibinin kimliğini; nüfus cüzdanı, pasaport veya eşdeğerli güvenilirliğe sahip diğer bir belgeye istinaden tespit etmelidir.

✓ Dolaylı tespit yöntemi

Sertifika hizmet sağlayıcı, sertifika talep edenlerin kimlik bilgilerini eğer daha önceden oluşturulmuş, Kanunun ve Yönetmeliğin aradığı koşulları (resmi belgeler) taşıyan veri bankaları aracılığıyla tespit edebilirse, yeniden yüzyüze kimlik tespiti yapmaktan kaçınabilir.

Elektronik sertifika kullanımının yaygınlaştırılması amacıyla, Yönetmelikte yapılacak düzenlemeyle her iki sistemin de işlemesine imkan verecek bir yapı ortaya konulmalıdır.

- *Sertifika hizmet sağlayıcının ve sertifika sahibinin imza oluşturma verileri*

Sertifika hizmet sağlayıcılarının ve alt sertifika otoritelerinin sertifikaları ve kapalı anahtarları, son kullanıcı sertifikalarının oluşturulması ve imza doğrulaması açısından çok önemlidir. Bu nedenle, uygulamada sertifika hizmet sağlayıcıların ve alt sertifika otoritelerinin, imza oluşturma verilerinin saklanması gerekmektedir. Elektronik imza

kullanımının güvenliğinin arttırılması amacıyla, sertifika hizmet sağlayıcılarının imza oluşturma verilerinin ve sertifikalarının bir yedeğinin Kurum tarafından saklanması Yönetmelikle öngörülebilir. Böylece sertifika hizmet sağlayıcının Kanuni yükümlülüklerini yerine getirmemesi ve olası bir uyuşmazlığın çıkması durumlarında Kurumun sakladığı sertifikadan ve kapalı anahtardan yararlanılabilir.

Sertifika hizmet sağlayıcıları, sertifikasyon hizmetlerinin güvenli bir şekilde yürütümünde gerekli olan felaketten kurtarma operasyonları için alt sertifika otoritesinin imza oluşturma verisinin yedeğini saklayabilir. Bu durum Kanunda belirtilen *"sertifika hizmet sağlayıcı imza oluşturma verisinin bir yedeğini alamaz"* hükmünün kapsamına girmemektedir. Bu hükümle düzenlenen son kullanıcının imza oluşturma verisidir. Ayrıca burada dikkat edilmesi gereken bir başka nokta ise; Kanunla yasaklanan konunun sertifika hizmet sağlayıcının, imza oluşturma verisini saklayamamasıdır; oysa bir başka kişi/kurum imza oluşturma verisinin yedeğini saklayabilir. Uygulamada bu durum, imza oluşturma verisi saklama hizmeti veren yedieminlerle ortaya çıkabilir. Böyle bir uygulama Kanuna aykırı olmayacağı gibi, yediemin ve sertifika sahibi arasındaki ilişki özel hukuk kapsamında değerlendirilecektir.

- *Sertifika sahibini bilgilendirme*

Kanuna göre sertifika hizmet sağlayıcının, son kullanıcıyı sertifika kullanımı, sağlanan hizmetler ve elektronik imza kullanımı konusunda bilgilendirme yükümlülüğü bulunmaktadır. Sertifika hizmet sağlayıcının, son kullanıcıya güvenli elektronik imza oluşturma aracı önerme yükümlülüğü de bulunduğu için, aracın kullanımı konusunda da son kullanıcıyı bilgilendirmelidir. Sertifika kullanımı ve hizmetler ile ilgili olarak vereceği bilgilendirme dahilinde, sertifika sahibinin sertifikasının ve sertifikada bulunan kimlik bilgilerinin , herkesin ulaşabileceği bir dizinde bulunması konusu da bulunmaktadır. Kanunun 12. maddesinde belirtildiği üzere, sertifikanın herkesin ulaşabileceği bir dizinde bulunması, ancak sertifika sahibinin açık rızasıyla mümkün olmaktadır. Bu durumda sertifika hizmet sağlayıcının konuyla ilgili sertifika sahibini bilgilendirme ve rızasının ne yönde olduğunu öğrenme yükümlülüğü bulunmaktadır.

Sertifika hizmet sağlayıcı, son kullanıcıyı imza oluşturma verisi konusunda bilgilendirmelidir. Sertifika sahibinin imza oluşturma verisini saklama yükümlülüğü konusunda, son kullanıcıya bilgi verilmelidir. Sertifika hizmet sağlayıcı, son kullanıcıya elektronik imzanın ve güvenli elektronik imzanın hukuki sonuçları hakkında bilgi vermelidir. Her iki çeşit elektronik imzanın da Kanun kapsamında hukuki değeri bulunmaktadır, ancak sadece güvenli elektronik imza elle atılmış imza ile aynı hukuki sonucu doğurmaktadır. Son kullanıcılar güvenli elektronik imzanın hukuki değeri hakkında bilgi sahibi olmalı ve bu imzayı kullandıklarında, imzaladıkları irade beyanlarıyla bağlı olacaklarını bilmelidirler.

Sertifika hizmet sağlayıcılarının, sertifikanın mali ve kullanım kısıtlamaları konusunda son kullanıcıyı bilgilendirme yükümlülüğü bulunmaktadır. Sertifikada bu kısıtlamaların bulunması durumunda, Kanuna göre sertifika sahibi bu kısıtlamaların kapsamı dışında bir işlem yaptığı takdirde, sertifika hizmet sağlayıcının yükümlülüğü bulunmamaktadır. Bu sebeple son kullanıcı sertifikanın hangi konularda ve ne kadar kısıtlandığı hakkında bilgilendirilmeli ve kısıtlama sonucunda ortaya çıkan sorumluluk matrisi kullanıcıya açıklanmalıdır.

Sertifika hizmet sağlayıcı, elektronik imza kullanımından doğan veya sertifika hizmet sağlayıcı ile sertifika sahibi arasında çıkan uyuşmazlıklarda başvurulabilecek alternatif uyuşmazlık çözüm yolları hakkında son kullanıcıyı bilgilendirmelidir[15].

Sertifika hizmet sağlayıcının, son kullanıcıyı sertifika iptal hizmetinin nasıl kullanılacağı ve imza doğrulama işleminin nasıl yapılacağı konusunda da bilgilendirme yükümlülüğü bulunmalıdır. Bu iki işlem sertifika hizmetinin düzgün işlemesi ve imza işleminin kullanıcı tarafından kullanılabilmesi için gereklidir.

- *Kayıtlar*

Sertifika hizmet sağlayıcılarının, sertifika hizmetlerinin yürütümü ve Kanundan doğan yükümlülüklerini yerine getirmek amacıyla tutması gereken üç çeşit kayıt vardır;

[15] Avukatlık Kanunu md. 35/a' da düzenlenen arabuluculuk (mediation) gibi.

1. Sertifika hizmet sağlayıcıları, verdikleri hizmetlere ve hizmetlerdeki değişikliklere ilişkin olarak kayıt tutmalıdır.

2. Sertifika hizmet sağlayıcıları, güvenlik sistemlerine, güvenlik sistemlerindeki değişikliklere ve Kuruma yaptıkları bildirim ve faaliyet raporlarına ilişkin olarak kayıt tutmalıdır.

3. Sertifika bilgileri, imzanın doğrulanması için gereken bilgiler, sertifikada bulunan sertifika sahibine ve sertifika hizmet sağlayıcıya ait kimlik bilgileri kayıt altına alınmalı ve saklanmalıdır.

Yukarıda bahsedilen hususlarda minimum kayıt süresi belirlenmelidir. Bu konuda hukuki uyuşmazlıktan önceki dönem ve hukuki uyuşmazlıktan sonraki dönem şeklinde bir ayrım yapılarak saklama süreleri şu şekilde belirlenebilir:

Hukuki Uyuşmazlıktan Önceki Dönemde: Bu konuda Borçlar Kanunu (BK) md. 125'te yer alan genel hükümden istifade edilebilir. Bu hükme göre; *"Bu Kanunda başka suretle hüküm mevcut olmadığı takdirde her dava on yıllık müruru zamana tabidir"*. Dolayısıyla her alacağın dava konusu yapılması için BK'nın öngördüğü genel zamanaşımı süresi 10 yıldır. Sertifikaların saklanması bakımından da, yapılan hukuki işlemlerin dava konusu yapılabilmeleri için aranan bu 10 yıllık süreden istifade edilebilir. BK md. 125'de öngörülen sürede dava konusu yapılmayan alacaklar, bu süre geçtikten sonra artık dava edilemeyecekleri için, ilgililer arasında hukuki anlamda uyuşmazlık çıkması ihtimali de yok demektir. Sertifikaların da olası hukuki ihtilaflar dikkate alındığında 10 yıl saklanması yerinde olacaktır.

Hukuki Uyuşmazlıktan Sonraki Dönemde: BK. Md. 125'de öngörülen sürede dava konusu yapılan alacaklar bakımından ise, sertifikaların saklanma süresi açısından İcra ve İflas Kanunu (İİK) md. 39/f. 1'deki hükümden yararlanılabilecektir. İİK. Md. 39/f.1'e göre; *"İlama müstenit takip son muamele üzerinden on sene geçmekle zamanaşımına uğrar"*. Buna göre bir dava sonucunda verilen mahkeme kararları bu

on yıllık süre zarfında icraya konulmalıdır. Aksi takdirde sürenin geçmesi halinde ilam (mahkeme kararı) zamanaşımına uğrayacak yani bir daha icrası istenemeyecektir.

Bu nedenle dava konusu yapılmış sertifikalar veya sertifikaların delil olarak kullanılacağı davalar bakımından, bu sertifikaların İİK. Md. 39/f.1 uyarınca mahkeme kararının verilmesinden itibaren 10 yıl saklanması gerekecektir.

Sonuç olarak yukarıdaki açıklamalar dikkate alındığında, kayıt saklama süresinin minimum 20 yıl olması mevcut hukuk sistemimiz açısından isabetli olacaktır.

- *Faaliyete son vermeyi bildirme usulü*

Faaliyetine son verecek sertifika hizmet sağlayıcıların durumu Kuruma ve kullanıcılarına bildirme zorunluluğu bulunmaktadır. Sertifika hizmet sağlayıcılarının güvenliği ve elektronik sertifika hizmetlerinin düzenli bir şekilde işlemesi için Kuruma yapılan faaliyete son verme bildiriminin yazılı formatta olması gerekmektedir. Bunun sonucu olarak sertifika hizmet sağlayıcının, elektronik ortamdan faaliyete son verme bildirimini yollaması mümkün olmayacaktır.

Kurum faaliyetine son verme talebini ileten sertifika hizmet sağlayıcısını ve faaliyetine son verme tarihini de ayrıntılı bir biçimde belirterek (gün, saat, saniye), Kurumun kendi web sitesinden duyurmalıdır.

Sertifika hizmet sağlayıcısının son kullanıcılara yapacağı, faaliyete son verme bildirimi elektronik ortamdan yapılabilmelidir. Bildirimin elektronik ortamdan yapılması durumunda, bildirimde sertifika hizmet sağlayıcının güvenli elektronik imzası bulunmalıdır. Sertifika hizmet sağlayıcılara, son kullanıcılara yapacağı bildirimin yazılı olarak yapma zorunluluğu getirilmemelidir. Çünkü böyle bir zorunluluk karşısında sertifika hizmet sağlayıcı yüz binlerce kişiye tebligat yapmak zorunda kalabilecektir.

- *Zaman Damgası ve Hizmetleri*

Zaman damgası hizmet sağlayıcısının tanımı Kanunla yapılmamıştır. Zaman damgası hizmet sağlayıcılar, verdikleri hizmetin teknik ve hukuki yönleri bakımından, Kanun kapsamında sertifika hizmet sağlayıcı sayılamazlar. Bu sebepten ötürü Yönetmeliğin tanımlar bölümünde, zaman damgası hizmet sağlayıcısının tanımı ayrıca yapılmalı ve böylece sertifika hizmet sağlayıcısından ayrı bir kurum olduğu hukuki olarak açıklığa kavuşturulmalıdır.

Zaman damgası da elektronik sertifika gibi bir teknolojik üründür ve yeterli güvenliğe sahip zaman damgasının tanımı teknik metinlerle yapılmalıdır. Bu sebepten ötürü zaman damgası ile ilgili gereksinimlerin belirlenmesinde, uluslararası standartlar referans gösterilmelidir. Yönetmeliğin bu bölümünde, standartların yer aldığı bölüme atıf yapılmalıdır.

3. Nitelikli Elektronik Sertifikaların İptal Edilmesi

- *Sertifika iptal talebi*

Sertifika hizmet sağlayıcısı, sertifika iptal talebi konusunda öncelikle, iptal talebinde bulunan kişinin sertifikayı iptal yetkisinin bulunup bulunmadığını tespit etmelidir. Sertifika iptal talebinde bulunabilecek yetkili kişiler sertifika sahibi veya sertifika sahibini temsil etmeye yetkili kişiler olabilir. Sertifika hizmet sağlayıcı sertifika iptal talebinde bulunan kişinin sertifikayı iptal yetkisinin bulunup bulunmadığını gerekli bilgi güvenliği yöntemlerini kullanarak tespit etmelidir (PIN sorgulama, kişisel veri kontrolü).

Sertifika iptal istemlerinin her zaman gelebilecek olması ve iptal işlemlerinde yaşanan gecikmelerin ağır hukuki ve mali zararlar doğurabilecek olması sebebiyle sertifika hizmet sağlayıcısı, sertifika iptal taleplerini karşılayabilmek için 7/24 saat hizmet verebilecek bir web sitesi ve telefon destek sistemi kurmalıdır.

- *Dizin hizmeti ve sertifika iptal listeleri*

Sertifika hizmet sağlayıcılarının kullanacakları sertifika dizin sunucuları ve yayınlayacakları sertifika iptal listeleri; sertifikaların başka bir sertifika sağlayıcıya devri söz konusu olduğunda ve karşılıklı işlerliğin sağlanması amacıyla, uluslararası standartlara uygun olmalıdır.

Yönetmeliğin Altıncı Bölümünde konuyla ilgili standartlar belirtilmeli ve bu bölümde Altıncı Bölüme atıf yapılmalıdır.

- *Sertifikaların ve sertifika iptal listelerinin devri*

Sertifikalar ve sertifika iptal listeleri Kanunun 8. ve 10. maddeleri uyarınca başka bir sertifika sağlayıcıya veya Kuruma devredilebilir veya Kurumun kararı uyarınca devredilme zorunluluğu doğabilir. Buna göre devir iki sebepten ortaya çıkabilir;

1. Sertifika hizmet sağlayıcının hizmetlerine kendisinin son vermesi

Sertifika hizmet sağlayıcısı, faaliyetine son vermek istediği takdirde, yayınlamış olduğu sertifikaları başka bir sertifika hizmet sağlayıcıya devretmek zorundadır. Başka bir sertifika hizmet sağlayıcının bulunmaması veya devri kabul etmemesi durumunda, sertifika hizmet sağlayıcı, Kanuna gör elindeki sertifikaları derhal iptal etmek zorundadır. Sertifikaların devredilmesi durumunda; sertifika hizmet sağlayıcısı, sertifikaları, dizin ve sertifika iptal listelerine ait URL'leri, sertifika sahiplerine ait kimlik bilgilerini ve belgelerini, devri kabul eden sertifika hizmet sağlayıcıya devretmek zorundadır.

2. Sertifika hizmet sağlayıcıların hizmetlerine Kurum tarafından son verilmesi

Sertifika hizmet sağlayıcının faaliyetlerine Kurum tarafından son verilmesi halinde, Kanuna göre Kurum, sertifikaların başka bir elektronik sertifika sağlayıcısına devredilmesine karar verir. Burada yönetmelikle açıklanması gereken durum; Kurumun kararında hangi sertifika

hizmet sağlayıcıya devir yapılacağının Kurum tarafından belirtilip belirtilmeyeceğidir. Bu doğrultuda Kurum sadece devir kararı verebilir veya hangi sertifika sağlayıcıya devir yapılacağını da kararında belirtebilir. Sertifika hizmet sağlayıcının faaliyetlerinin kurum tarafından durdurulması veya faaliyetlerine son verilmesi durumunda, piyasada faaliyet gösteren başka bir sertifika sağlayıcının bulunmaması veya devri kabul etmemesi halinde Kurum sertifikaları ve sertifika iptal listelerini sertifika hizmet sağlayıcıdan devralmalıdır. Böylece Kurum elektronik imzalar için güvenli bir ortam sağlamış olacak ve son kullanıcıların sertifika hizmet sağlayıcıları karşısındaki risklerini azaltmış olacaktır.

4. Yabancı Elektronik Sertifikalar

Kanuna göre yabancı sertifikaların ülke içinde nitelikli sertifika sayılabilmeleri için ülke içinde yerleşik bir sertifika hizmet sağlayıcı tarafından garanti edilmeleri gerekmektedir. Garanti verme işlemi ;garanti veren sertifika hizmet sağlayıcısı ile yabancı sertifika hizmet sağlayıcısının aralarında çapraz sertifikasyon (cross-certification) yapmasıyla mümkün olacaktır. Çapraz sertifikasyon iki servis sağlayıcının aralarında sözleşme yapmasıyla mümkün olacak ve bu ilişkiden doğan hukuki çerçeve sözleşme hükümleri ve genel hükümler kapsamında ortaya çıkacaktır. Son kullanıcı açısından ise, yükümlülük garanti veren sertifika hizmet sağlayıcıdadır. Yabancı sertifikalara garanti verme işlemi için çapraz tanıma (cross-recognition) işlemi kullanılamamaktadır, zira çapraz tanımada ülke içinde yerleşik bir sertifika sağlayıcı yabancı sertifikaları garanti etmemektedir. Ancak çapraz tanıma işlemi, güvenilir üçüncü taraf aracılığıyla yapılıyor ve bu üçüncü taraf ülke içinde yerleşik bulunuyorsa bu sistem de, yabancı sertifikaların garanti edilmesi için kullanılabilir. Çapraz tanıma (cross – recognition)'nın ülke içinde elektronik sertifika hizmet sağlayıcılarının yarattıkları güvenlik alanlarının entegrasyonunu ve karşılık işlerliliğinde maliyet etkin, uygulanması kolay ve çabuk bir yöntem olması nedeniyle tercih edilebilir. Telekomünikasyon Kurumu özellikle sertifikasyon pazarını düzenleme ve pazarı yönlendirme misyonun bir gereği olarak ülke içinde dolaşımda olan ve kanuna tabi elektronik sertifika hizmet sağlayıcıları tarafından üretilen sertifikaların karşılıklı işlerliğini sağlamak adına yapacağı düzenlemelerde (Örn. bu konuda yayınlayacağı tebliğ, sirkü, karar v.b. hukuksal

enstrümanlarda) çapraz tanımının benimsenmesi yolunda elektronik sertifika hizmet sağlayıcılarına yükümlülük getirebilir.

5. Diğer Hükümler

- *Faaliyet raporu*

Kurum sertifika hizmet sağlayıcıların faaliyetleri ile ilgili bilgi edinmek için, sertifika hizmet sağlayıcılardan periyodik olarak faaliyet raporu istemelidir. Yönetmelikle bu faaliyet raporunun içeriğinde bulunması gerekenler belirlenmeli ve bu raporun hangi sıklıkla isteneceği ortaya konulmalıdır. Faaliyet raporu matbu bir belge olarak Kurum tarafından hazırlanabilir ve sertifika hizmet sağlayıcıların bu formu doldurması istenebilir.

- *Kurum Tarafından Rapor Düzenlenmesi*

Telekomünikasyon Kurumu, sektördeki durumu tespit etmek amacıyla, bir önceki yıla ait olmak üzere,

a) Kendisine yapılan, sertifika hizmet sağlayıcı olarak faaliyet gösterme bildirimi sayısını,

b) Olumlu cevaplanarak faaliyete geçen sertifika hizmet sağlayıcı sayısını,

c) Sertifika hizmet sağlayıcı veya Kurum tarafından faaliyetine son verilen sertifika hizmet sağlayıcıları ve sayılarını,

d) Sertifika hizmet sağlayıcılar arasında veya Kurum tarafından başka bir sertifika hizmet sağlayıcıya tevdi edilen sertifika ve hizmet devirlerini,

e) İptal edilen sertifikaların sayısını,

gösterir bir genel rapor hazırlamalıdır. Bu rapor sertifika hizmet sağlayıcıların hazırlayıp, kendisine gönderdiği faaliyet raporları ile birlikte her yıl Nisan ayının sonuna kadar Türkiye Büyük Millet Meclisine gönderilmelidir. Raporlar, bu süreci takip eden iki ay içinde Türkiye

Büyük Millet Meclisi Başkanlığınca ve Kurum tarafından kendi web sayfasından eş zamanlı olarak kamuoyuna açıklanmalıdır.

- *Yaptırımlar (idari para cezaları)*

Cezaların kanuniliği ilkesi gereğince, yönetmelikle kanunun öngörmediği cezalar getirilmemelidir. Bu sebeple yönetmelikle düzenlenen konuların yaptırımına ilişkin idari cezalarda kanunun ilgili maddesi çerçevesinde idari cezalar düzenlenmeli ve kanunun ilgili maddelerine atıf yapılmalıdır.

- *Hüküm bulunmayan haller*

Kanunda ve Yönetmelikte hüküm bulunmayan hallerde, genel hükümler ve Kurumun çıkartacağı tebliğler geçerli olacaktır.

- *Geçici hükümler*

Yönetmeliğin bu kısmında, Kanun ve Yönetmelik yürürlüğe girmeden önce yayınlanmış olan sertifikaların durumları ile ilgili hükümler bulunacaktır. Buna göre Kanunun ve Yönetmeliğin yürürlüğe girmesinden önce yayınlanmış olan ve Kanunun aradığı nitelikli elektronik sertifika koşullarına sahip elektronik sertifikalar, yürürlükten itibaren nitelikli elektronik sertifika sayılacaklardır.

6. Mali Mesuliyet Sigortası

5070 Sayılı Elektronik İmza Kanununun *"Yönetmelik"* kenar başlıklı 20. maddesinde Telekomünikasyon Kurumu tarafından yönetmelikle düzenlenecek maddeleri arasında Kanunun 6, 7, 8, 10, 11 ve 14. maddeleri gösterilmiştir. Kanunun *"Hukuki Sorumluluk"* kenar başlıklı 13. maddesinin 5. fıkrasında ise; Telekomünikasyon Kurumu tarafından Yönetmelikle düzenlenmesi öngörülen diğer bir konu ise *"Sertifika Mali Mesuliyet Sigortası"*dır.

Ancak 20. madde de yönetmelik ile düzenlenecek maddeler arasında açıkça md. 13/f.5'e atıf yapılmadığından, Kurum tarafından 20. maddede işaret edilen 6 maddeye ilişkin olarak hazırlanacak yönetmeliğin içinde, sertifika mali mesuliyet sigortasına ilişkin yönetmeliğin yer alması hukuk tekniği açısından doğru değildir.Kurumun bu noktaya özel olarak hassasiyet göstermesi ve sertifika mali mesuliyet sigortasına ilişkin yönetmeliği ayrıca yayınlaması gerekmektedir.

Mali mesuliyet sigortası ile ilgili düzenleme yaparken, sertifika hizmet sağlayıcıların sertifika üretiminden, sertifika hizmetlerinin yürütümünden ve sertifika sahibinin kimlik bilgilerinin hatalı kayıt edilmesinden kaynaklanacak risklerin giderilmesi göz önünde bulundurulmalıdır.

ÜÇÜNCÜ BÖLÜM – ELEKTRONİK İMZA KANUNUNUN UYGULANMASINA YÖNELİK USUL VE ESASLARIN AÇIKLANDIĞI YÖNETMELİK ŞABLONU TASLAĞI

5070 SAYILI ELEKTRONİK İMZA KANUNUNUN UYGULANMASINA İLİŞKİN USÛL VE ESASLAR HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM
Genel Hükümler

- **Amaç**

Yönetmeliğin amacı, "elektronik imza araçlarının, yabancı elektronik sertifikaların hukukî ve teknik yönlerine ve elektronik sertifika hizmet sağlayıcılarının yükümlülüklerine ilişkin esasları düzenlemek" olmalıdır.

- **Kapsam**

Yönetmelik, *"elektronik imza araçlarının ve yabancı elektronik sertifikaların hukuki ve teknik yönlerine ilişkin gereksinimleri ve elektronik sertifika hizmet sağlayıcılarının yükümlülüklerine ilişkin usul ve esasları"* kapsamalıdır.

- **Hukuki Dayanak**

Yönetmelik 5070 sayılı Kanunun 20. maddesinde belirtildiği üzere 6, 7, 8, 10, 11, 14 maddelerine dayanılarak hazırlanmalıdır.

- **Tanımlar**

Yönetmelikte, Elektronik İmza Kanunu'nda yapılan tanımlara ek olarak aşağıda belirtilen tanımların Yönetmelikte yer alması Yönetmeliğin kurgusu açısından gereklidir.

Bildirimi inceleyecek kurul *:* Sertifika hizmet sağlayıcıların faaliyete başlama ve faaliyete son verme bildirimlerini inceleyecek, sertifika hizmet sağlayıcılarının faaliyetlerinin devamı sırasında faaliyete başlama bildiriminde belirttiği niteliklerin denetimini yapacak Kurum bünyesinde oluşturulmuş gerekli teknik, hukuki ve denetim bilgisine sahip personelden oluşan Kurul

Alt Sertifika Otoritesi: Sertifika hizmet sağlayıcısının kök sertifikası altında bulunan ve sertifika zincirinde son kullanıcı sertifikaları ile kök sertifika arasında yer alan kurum/kişi

Kayıt Otoritesi: Sertifika hizmet sağlayıcısının yayınlayacağı nitelikli sertifikalarda gerekli kimlik bilgilerinin kayıtlarını yapan ve kimlik tespitinde bulunan, sertifika hizmet sağlayıcıyla arasında sözleşme ilişkisi bulunan gerçek veya tüzel kişiler

Zaman Damgası Hizmet Sağlayıcısı: Sadece zaman damgası hizmeti veren gerçek veya tüzel kişiler

Sertifika İptal Listesi: Sertifika hizmet sağlayıcının; iptal edilen sertifikaların bilgilerinin yer aldığı, sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkan veren kayıt

Dizin ve Sertifika İptal Listesi Hizmet Sağlayıcısı: Sadece sertifika dizini hizmeti ve sertifika iptal listesi hizmeti veren gerçek veya tüzel kişiler

Faaliyet Raporu: Sertifika hizmet sağlayıcılarının faaliyetlerinin yürütümüyle ilgili olarak Kurumu bilgilendirmeye yönelik, sertifika hizmet sağlayıcı tarafından Kuruma periyodik aralıklarla sunulan doküman

- **İlkeler**

- ✓ Serbest rekabet ortamının oluşturulması,
- ✓ Tüketici haklarının korunması,
- ✓ Ülkede elektronik sertifika ve elektronik imza kullanımının yaygınlaştırılması

İKİNCİ BÖLÜM
Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları

- **Kurumun güvenli elektronik imza oluşturma araçlarını tanımlaması**

  - ✓ Türkiye'de güvenli elektronik imza oluşturma ve doğrulama araçlarını piyasaya sürecek satıcıların Kurum'un hazırladığı matbu formlarla Kurum'a bildirim yapma zorunluluğu

  - ✓ Bildirim sırasında, Yönetmelikle belirtilen güvenli elektronik imza aracı standartlarının yerine getirildiğini gösteren belgenin Kurum'a tevsiki

  - ✓ Kurum tarafından uygun bulunan araçların, Kurum'un web sitesinde kamuoyuna duyurulması

- **Elektronik imza oluşturma aracı sahibinin sorumluluğu**

  - ✓ Araç sahibinin aracın güvenliğini sağlamakla ilgili sorumluluğu (software)

  - ✓ Araç sahibinin aracın güvenliğini sağlamakla, aracını kaybetmemek için yeterli özeni göstermekle ilgili sorumluluğu (hardware)

  - ✓ Araç sahibinin imza oluşturma verisini başkasına kullandırmamakla ilgili sorumluluğu

✓ Software araçların güvenli sayılabilmesi için, yazılımın lisanslı olması zorunluluğu

- **PIN**

✓ Yazılım bazlı elektronik imza oluşturma araçlarının aktif hale gelebilmesi için PIN kodu girilmesi zorunluluğu

✓ Yazılım bazlı imza oluşturma aracının, çok işlevli bir programın (multi-application terminal) parçası olması durumunda, imza oluşturma fonksiyonuna geçilmesi için ayrı PIN girilmesi

- **Sertifika hizmet sağlayıcıların kullanacağı teknik araçlar**

✓ Sertifika hizmet sağlayıcıların kullanacağı araçların sağlaması gereken teknik standartlar, Yönetmeliğin Altıncı Bölüm'ünde belirtilecektir.

- **Güvenli elektronik imza oluşturma ve doğrulama araçlarına ilişkin standartlar**

✓ Sertifika sahiplerinin kullanacağı araçların sağlaması gereken teknik standartlar, Yönetmeliğin Altıncı Bölüm'ünde belirtilecektir.

ÜÇÜNCÜ BÖLÜM
Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri

- **SHS'nin asgari hizmetleri**

1. Kendi kök sertifikası altında nitelikli elektronik sertifika yayınlama
2. 7/24 teknik destek (web sayfası, çağrı merkezi)
3. Sertifika politikası ve sertifika uygulama hükümleri belgelerinin hazırlanması ve yayınlanması
4. Anahtar ve sertifika yaşam döngüsü kontrolleri
5. Personelin niteliği
6. Operasyon merkezinin fiziksel ve çevre güvenliği
7. Sistem izleme ve denetleme

- **Bildirim**

✓ Bildirim, Kurumun hazırladığı matbu formlar yoluyla yapılmalıdır

✓ Bildirimde sertifika hizmet sağlayıcıların yerine getirmesi gereken şartlar Webtrust ve ETSI gibi uluslararası standartlara dayanmalıdır

✓ Bildirim sadece elden teslim yoluyla yapılmalıdır

✓ Kuruma yapılacak başvuruları değerlendirecek, "Başvuru İnceleme Kurulu" tanımlanmalıdır

✓ Başvuru İnceleme Kurulu'nun yetkileri ve bu Kurulda çalışacak personelin nitelikleri belirlenmelidir

- **Kurumun sertifika hizmet sağlayıcılardan talep edeceği ücretler**

✓ Kurum inceleme, denetleme ve kamuoyunu bilgilendirme görevlerini yerine getirmek için sertifika hizmet sağlayıcılardan ücret talep etmelidir

✓ Ücretler, bildirim inceleme ücreti ve denetleme ücreti olarak belirlenebilir

✓ Kurum güvenli elektronik imza oluşturma ve doğrulama aracı satıcılarından, ürün kaydı ve kamuoyuna duyurma ücreti talep etmelidir

- **Faaliyete son verme, faaliyeti durdurma**

✓ Kurum sertifika hizmet sağlayıcısının faaliyetine son verdiğini veya durdurduğunu kendi web sitesinden kamuoyuna duyurmalıdır

✓ Sertifika hizmet sağlayıcının faaliyetlerinin devamı sırasında Kanunda ve Yönetmelikte belirtilen şartları yerine getirip getirmediğinin tespiti, sertifika hizmet sağlayıcı tarafından Kuruma periyodik aralıklarla gönderilen "faaliyet raporları" ve Kurumun yaptığı denetimlerle incelenmelidir

✓ Kurumun, sertifika hizmet sağlayıcısının faaliyetine son vermesi veya durdurması halinde sertifika hizmet sağlayıcının yayınlamış olduğu sertifikalar ve sertifika iptal listelerinin devredilme şekli Dördüncü Bölümdeki Dizin ve İptal Hizmetlerinin Devri kısmındaki hükümlere göre düzenlenmelidir

- **Sertifika ücretleri alt ve üst sınırları**

✓ Kurum tarafından belirlenecek "sertifika ücretleri alt ve üst sınırları" maliyet bazlı hesaplama yöntemiyle ortaya konulmalıdır.

✓ Alt ve üst sınırlar belirlenirken, Türkiye'de elektronik sertifika pazarının oluşmamış olması, piyasaya girecek hizmet sağlayıcıların engellenmemesi, elektronik sertifika ve elektronik imza kullanımının özendirilmesi gibi hususlar göz önünde bulundurulmalıdır.

✓ Sertifika fiyatlarının piyasaya sürülme sayılarına göre büyük farklılıklar arz etmesi ve sertifika çeşitleri arasında farklılıklar bulunması sebebiyle, sertifika alt ve üst sınırları geniş ölçekle tespit edilmelidir.

- **Sertifika hizmet sağlayıcının personelinin sahip olması gereken nitelikler**

✓ Sertifika hizmet sağlayıcıların çalıştıracağı teknik personelin sahip olması gereken spesifik teknik bilgiler şu konularda olmalıdır;

1. İleri derecede bilgisayar bilgisi
2. Güvenlik teknolojisi, kriptografi, elektronik imza ve açık anahtarlı altyapı
3. Uluslararası teknik standartlar ve özellikle değerlendirme standartları
4. Donanım ve yazılım

✓ Sertifika hizmet sağlayıcı, personelinin niteliklerini Kuruma lisans, yüksek lisans, sertifika gibi belgelerle kanıtlamalıdır

- **Sertifika kayıtları ve kimlik tespiti**

✓ Yönetmelikle sertifika kayıtlarının hem doğrudan hem de dolaylı yolla yapılmasına imkan sağlayacak bir düzenleme yapılmalıdır

✓ Sertifika hizmet sağlayıcı talep sahibinin kimliğini; nüfus cüzdanı, pasaport veya eşdeğerli güvenilirliğe sahip diğer bir belgeye istinaden tespit etmelidir.

- **Sertifika hizmet sağlayıcının ve sertifika sahibinin imza oluşturma verileri**

✓ Sertifika hizmet sağlayıcıları, imza oluşturma verilerinin bir kopyasını Kurum'a devretmelidir.

✓ Felaketten kurtarma operasyonları için sertifika hizmet sağlayıcı, alt sertifika otoritesinin imza oluşturma verisinin yedeğini saklayabilir.

✓ Sertifikaların ve imza oluşturma verisinin, son kullanıcıya ulaştırılması konusu düzenlenmelidir. Burada

✓ Soft sertifikalar elektronik ortamda ve depolama araçları(cd, disket, v.s.) aracılığıyla son kullanıcıya ulaştırılabilmelidir

✓ sertifikaların donanım(smart card, usb token) ile birlikte verilmesi durumunda sertifikaların son kullanıcıya teslimine kadar sorumluluk sertifika hizmet sağlayıcıda olmalıdır

- **Sertifika sahibini bilgilendirme**

Sertifika hizmet sağlayıcı aşağıdaki konularda son kullanıcıya bilgi vermek zorundadır;

✓ Sertifika kullanımı, sağlanan hizmetler ve elektronik imza kullanımı

✓ Güvenli elektronik imza oluşturma aracının kullanımı

✓ Sertifika sahibinin imza oluşturma verisini saklama yükümlülüğü

✓ Elektronik imzanın ve güvenli elektronik imzanın hukuki sonuçları

✓ Sertifikanın mali ve kullanım kısıtlamaları

- ✓ Elektronik imza kullanımından doğan veya sertifika hizmet sağlayıcı ile sertifika sahibi arasında çıkan uyuşmazlıklarda başvurulabilecek alternatif uyuşmazlık çözüm yolları

- ✓ Sertifika iptal hizmetinin kullanılması

- ✓ imza doğrulama işlemi

- **Kayıtlar**

Sertifika hizmet sağlayıcıları aşağıdaki hususlarda kayıt tutmalıdır;

- ✓ Sağladıkları hizmetler ve hizmetlerdeki değişiklikler

- ✓ Güvenlik sistemleri ve güvenlik sistemlerindeki değişiklikler

- ✓ Kuruma yaptıkları bildirim ve faaliyet raporları

- ✓ Sertifika bilgileri, imzanın doğrulanması için gereken bilgiler, sertifikada bulunan sertifika sahibine ve sertifika hizmet sağlayıcıya ait kimlik bilgileri ve belgeleri

- ✓ Yukarıda bahsedilen hususlarda minimum kayıt süresi belirlenmelidir. Kayıtlar en az yirmi yıl süreyle saklanmalıdır.

- **Faaliyete son vermeyi bildirme usulü**

- ✓ Kuruma yapılan faaliyete son verme bildirimi yazılı formatta olmalı ve elektronik ortamdan bildirimin yollanması mümkün olmamalıdır.

✓ Kurum faaliyetine son verme talebini ileten sertifika hizmet sağlayıcısını, Kurumun web sitesinden duyurmalıdır.

✓ Sertifika hizmet sağlayıcısının son kullanıcılarına yapacağı, faaliyete son verme bildirimi güvenli elektronik imzasının bulunması şartıyla elektronik ortamdan yapılabilmelidir.

- **Zaman Damgası ve Hizmetleri**

✓ Zaman damgası hizmeti verecek sertifika hizmet sağlayıcının tanımı, Tanımlar bölümünde yapılmalıdır.

✓ Zaman damgası ile ilgili teknik gereksinimler için Altıncı Bölüm'e atıf yapılmalıdır.

DÖRDÜNCÜ BÖLÜM
Nitelikli Elektronik Sertifikaların İptal Edilmesi

- **Sertifika iptal talebi**

✓ Sertifika hizmet sağlayıcısı, sertifika iptal talebinde bulunan kişinin sertifikayı iptal yetkisinin bulunup bulunmadığını gerekli bilgi güvenliği yöntemlerini kullanarak tespit etmelidir.

✓ Sertifika hizmet sağlayıcısı, sertifika iptal taleplerini karşılayabilmek için 7/24 hizmet verebilecek bir web sitesi ve telefon destek sistemi kurmalıdır.

- **Dizin hizmeti ve sertifika iptal listeleri**

Sertifika hizmet sağlayıcılarının kullanacakları sertifika dizin sunucuları ve yayınlayacakları sertifika iptal listeleri uluslararası standartlara uygun olmalıdır. Yönetmeliğin Altıncı Bölümünde konuyla ilgili standartlar belirtilmeli ve bu maddede Altıncı Bölüme atıf yapılmalıdır.

- **Sertifikaların ve sertifika iptal listelerinin devri**

✓ Sertifikaların devredilmesi durumunda sertifika hizmet sağlayıcısı, sertifikaları, dizin ve sertifika iptal listelerine ait URL'leri, sertifika sahiplerine ait kimlik bilgilerini ve belgelerini, devri kabul eden sertifika hizmet sağlayıcıya devretmek zorundadır.

✓ Sertifika hizmet sağlayıcının faaliyetlerinin kurum tarafından durdurulması veya faaliyetlerine son verilmesi durumunda, piyasada faaliyet gösteren başka bir sertifika sağlayıcının bulunmaması veya devri kabul etmemesi halinde Kurum sertifikaları ve sertifika iptal listelerini sertifika hizmet sağlayıcıdan devralmalıdır.

BEŞİNCİ BÖLÜM
Yabancı Elektronik Sertifikalar

✓ Garanti veren sertifika hizmet sağlayıcısı ile yabancı sertifika hizmet sağlayıcısı aralarında çapraz sertifikasyon (cross-certification) sözleşmesi yapmalıdırlar.

ALTINCI BÖLÜM
Teknik Hususlar

Bu bölümde elektronik imza ile ilgili uluslararası standartlar bulunmalıdır. Yer verilecek standartlar şu konularla ilgili olmalıdır,

- ✓ Sertifika hizmet sağlayıcıların kullanacağı teknik araçlar ve güvenli elektronik imza oluşturma araçları (CWA 14167-1, CWA 14167-2, CWA 14167-3)

- ✓ Sertifika sahiplerinin kullanacağı güvenli elektronik imza oluşturma araçları (CWA 14169)

- ✓ Zaman damgası (ETSI TS 101 861 v 1.2.1)

- ✓ Dizin hizmeti ve sertifika iptal listeleri

(1988 CCITT (ITU-T) x.500/ISO IS9594)

(RFC 2587 Internet X.509 PKI LDAPv2 Schema)

(RFC 2459 Internet X.509 PKI Certificate and CRL profile)

(RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for dynamic directory service)

YEDİNCİ BÖLÜM
Diğer Hükümler

- **Faaliyet raporu**

✓ Kurum sertifika hizmet sağlayıcıların faaliyetleri ile ilgili bilgi edinmek için, sertifika hizmet sağlayıcılardan periyodik olarak faaliyet raporu istemelidir.

✓ Faaliyet raporunun içeriğinde bulunması gerekenler belirlenmeli ve bu raporun hangi sıklıkla isteneceği ortaya konulmalıdır.

✓ Faaliyet raporu matbu bir belge olarak Kurum tarafından hazırlanmalıdır

- **Kurum tarafından rapor düzenlenmesi**

✓ Telekomünikasyon Kurumu, sektördeki durumu tespit etmek amacıyla, bir önceki yıla ait olmak üzere, sertifika ve elektronik imza kullanımı hakkında bir rapor yayınlamalıdır

- **Yaptırımlar (idari para cezaları)**

✓ Kanunun ilgili maddesi çerçevesinde idari cezalar düzenlenmeli ve kanunun ilgili maddelerine atıf yapılmalıdır.

- **Hüküm bulunmayan haller**

✓ Kanunda ve Yönetmelikte hüküm bulunmayan hallerde, genel hükümler ve Kurumun çıkartacağı tebliğler geçerli olacaktır.

- **Geçici hükümler**

  ✓ Yönetmeliğin yürürlüğe girmesinden önce yayınlanmış olan nitelikli elektronik sertifika gereksinimlerine sahip elektronik sertifikalar yürürlükten itibaren nitelikli elektronik sertifika sayılacaklardır.

- **Yürürlük**
- **Yürütme**

DÖRDÜNCÜ BÖLÜM – SONUÇ VE DEĞERLENDİRME

5070 sayılı Kanunun eksikliklerine rağmen, doğru kurgulanmış bir Yönetmelikle uygulamada pek çok sorunun aşılabileceğini yaptığımız bu çalışma ile ortaya koyduğumuzu düşünüyoruz. Raporda üzerinde özellikle durulan güvenli elektronik imza araçlarıyla ilgili hükümler ve sertifika hizmet sağlayıcıların yerine getirmesi gereken teknik ve hukuki gereksinimler ile sertifika hizmet sağlayıcı kavramının açıklığa kavuşturulması gibi konulara Kurumun hazırlayacağı Yönetmelikte özellikle hassasiyet göstermesi gerekmektedir. Kurum, Elektronik İmza Koordinasyon Kurulu'nun oluşturulması ve çalışmalar sırasında gösterdiği tutum ile sektörün ve akademik camianın görüşlerine önem verdiğini ve bu yasal süreçte mümkün olan en geniş katılımla şeffaflığın sağlanmasına çalıştığını tüm kamuoyuna göstermiştir. Hukuk Çalışma Grubu Raporu Yazarları olarak Kurum'dan beklentimiz, Yönetmelik taslağının hazırlanması sürecinde ve taslağın hazırlanmasından sonra da aynı tutumunu devam ettirmesidir. Yukarıda da belirtildiği gibi kurgusu iyi oluşturulmuş bir Yönetmelikle, Kanunun yanlış yorumlanmasından doğabilecek aksaklıklar engellenecek ve ülkede doğru işleyen bir elektronik sertifika piyasasının oluşumu sağlanabilecektir.

Elektronik sertifika pazarının gelişimi yalnızca sertifikasyon hizmetlerinin sunulmasının belirli kural ve şartlar dahilinde yürütülmesine bağlı değildir. Bunun yanında sertifikasyon pazarını destekleyecek denetim sistemleri hizmetleri, donanım, uygulama ve yazılımların da eş zamanlı olarak bu pazarın gelişimini destekleyecek bir şekilde piyasaya sürülmesini teşvik etmek, düzenleyici otoritenin en önemli sorumluluklarından biridir.

Kamu Kurumları ile özel sektör kuruluşları arasında 5070 Sayılı Kanunun 21. maddesi ile yaratılan rekabete aykırı durumun bir an önce bir kanun değişikliği ile giderilmesi gerekmektedir. Düzenleyici otoritenin bu kanun değişikliği gerçekleştirilene kadar maddenin yaratacağı rekabete aykırı olabilecek durumları engellemek adına sertifikasyon hizmetleri pazarını düzenleyecek ve özel sektör yatırımlarını dışlayıcı durumlar yaratmayacak çözümleri yetkili makamlara sunmak ve bu çözümlerin takipçisi olarak kamuoyunu bilgilendirmek gibi bir misyon da yüklenmelidir.

Kurumun elektronik imza ile ilgili sorumluluğu Yönetmeliğin hazırlanması ile son bulmayacaktır. Alt Yapı Çalışma Grubu'nun raporunda yer alan, kamu kurumlarında elektronik imza kullanımı konulu anketin sonuçlarından da açıkça anlaşıldığı üzere, kamuda elektronik imza ile ilgili bilgi eksikliği bulunmaktadır. Ayrıca bu kurumların hepsi kısa vadede, elektronik imza kullanımı gerektiren uygulamaları kendi bünyelerinde başlatmayı düşünmektedirler. Bu sebeplerden dolayı, kamu kurumlarının yöneticilerinin ve personelinin acil olarak elektronik imzanın hukuki ve teknik yönleri hakkında eğitilmesi gerekmektedir. Ayrıca e-devlet hedefine ulaşılması ve kamuda elektronik imza kullanımının arttırılması amacıyla kamu kurumlarında elektronik imza uygulamaları içeren uygulama projelerinin geliştirilmesi ve bu projelerin hayata geçirilmesi gerekmektedir.

Kamu kurumlarının yanı sıra, özel sektör ve toplumun da konuyla ilgili bilinçlendirilmesi gerekmektedir. Bilindiği üzere elektronik imza sistemi, bilgi toplumunun alt yapısını oluşturan en önemli uygulamalardan biridir. Vatandaşlar arasında elektronik imza kullanımının yaygınlaştırılması ile de e-ticaret ve e-devlet işlemlerinden sağlanacak faydalar en yüksek düzeye getirilecektir.

EK – 1 : AVUSTURYA, ALMAN, İSVEÇ ve İSVİÇRE ELEKTRONİK İMZA KANUNLARININ ve YÖNETMELİKLERİNİN 5070 SAYILI TÜRK ELEKTRONİK İMZA KANUNUNUN 20. MADDESİNDE YÖNETMELİKLE DÜZENLENMESİ ÖNGÖRÜLEN 6, 7, 8, 10, 11 ve 14. MADDELERİNİ KARŞILAYAN HÜKÜMLERİ

AVUSTURYA İMZA KANUNU ve YÖNETMELİĞİ

1. 5070 Sayılı Kanun md. 8: Sertifika Hizmet Sağlayıcı = Avusturya İmza Kanunu md. 6,7,8.

3. Bölüm

Sertifika Hizmet Sağlayıcı

Sertifika Hizmet Sağlayıcının Faaliyeti

§ 6 bir sertifika hizmet sağlayıcının faaliyete başlaması ve faaliyetini icra etmesi özel bir onaya tabi değildir.

Sertifika hizmet sağlayıcı faaliyete başladığını gecikmeksizin denetim Makamına (md. 13) bildirmek zorundadır. Sertifika hizmet sağlayıcı denetim makamına en geç faaliyete geçtiği tarihte veya hizmet değişikliği durumunda, kullandığı teknik bileşenler ve yöntemler de dahil olmak üzere sunduğu imza ve sertifika hizmetlerine ilişkin olarak bir güvenlik taslağı (konsept) ve ayrıca sertifikalandırma taslağı ibraz etmelidir.

Güvenli elektronik imza yöntemleri sunan bir Sertifika hizmet sağlayıcısı, bu kanun ve bu kanuna istinaden çıkartılan yönetmeliğin aradığı güvenlik koşullarına riayet ettiğini (yerine getirdiğini) bu güvenlik taslağında belirtmelidir.

Sertifika hizmet sağlayıcısı sertifikalandırma ve güvenlik taslağında belirttiği hususları hem faaliyete başlama hem de faaliyetinin icrası sırasında yerine getirmek durumundadır.

Sertifika hizmet sağlayıcısı usulüne uygun olarak ve güvenlik ve sertifikalandırma taslağındaki husulara ilişkin olarak yürüttüğü faaliyetini artık bu şekilde yürütmesini imkansız kılan tüm sebepleri gecikmeksizin denetim makamına bildirmek zorundadır.

Sertifika tanzim eden sertifika hizmet sağlayıcısı, güvenlik taslağında listeleme ve iptal hizmetlerinin hangi formda yürütülüp yürütülmeyeceğini de belirtmelidir.

Sertifika hizmet sağlayıcısı sertifikasını, sadece sertifika hizmetlerinin yerine getirilmesi için kullanabilecektir.

Nitelikli Sertifika İçin Sertifika Hizmet Sağlayıcısı

§ 7 Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcısı,

1. kendisi tarafından sunulan imza ve sertifikalandırma hizmetleri bakımından gerekli güvenilirliğe sahip olduğunu göstermek,
2. hızlı ve güvenli bir fihrist hizmeti, bunun gibi çabuk ve hızlı bir iptal hizmeti verdiğini garanti etmek,
3. nitelikli sertifikada ve ayrıca fihrist ve iptal hizmetlerinde zaman damgası kullanmak ve her halukarda nitelikli bir sertifikanın tanzim edildiği ve iptal edildiği zamanın tartışmasız olarak tespit edileceğini garanti etmek,
4. kendisi için nitelikli bir sertifika tanzim edilen kişinin kimliğini ve gerekirse özellikle hukuken önemli diğer özelliklerini resmi fotoğraflı bir kimlik belgesine istinaden güvenilir bir biçimde kontrol etmek,

5. sunulan hizmetin gerektirdiği branş bilgisine, tecrübeye ve yeteneklere sahip, özellikle yönetim kabiliyeti ve ayrıca elektronik imza teknolojisi ve ilgili güvenlik yöntemleri konusunda ehliyetli güvenilir personel çalıştırmak ve kabul edilen (benimsenen) normlara uygun idari ve yönetim prosedürlerine riayet etmek,
6. bu kanun ve bu kanuna istinaden çıkartılan yönetmeliğin aradığı koşulları yerine getirebilmek, ayrıca tazminat taleplerini karşılamak, yine mali mesuliyet sigortası tesis edebilmek için, yeterli mali kaynaklara sahip olmak,
7. özellikle bir dava sırasında sertifikalandırmanın ispatlanabilmesi için, nitelikli bir sertifika hakkındaki ilgili tüm durumları, kullanım amacı için uygun bir süre zarfında –gerekirse elektronik olarak da- kaydetmek
8. imza sahibinin imza oluşturma verisinin ne sertifika hizmet sağlayıcısı ne de üçüncü kişiler tarafından kaydedilmemesi veya kopyalanmaması için gerekli tedbirleri almak

zorundadır.

Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcısı, imza ve sertifika hizmetleri, sertifikaların hazırlanması ve kaydedilmesi için; tahrifatlara (değiştirmelere) karşı korumalı, teknik ve kriptografik güvenliği sağlanmış güvenilir sistem, ürün ve yöntemleri kullanmak zorundadır. Sertifika hizmet sağlayıcı ayrıca özellikle imza oluşturma verilerinin saklı tutulmasını sağlayacak, nitelikli sertifikaya ilişkin verilerin farkına varılmadan tahrif ve sahtekarlıklara maruz kalmasını önleyecek ve bu sertifikanın sadece imza sahibinin rızası ile açıkça (resmi olarak) geri alınabilmesini sağlayacak tedbirleri almak zorundadır. İmza oluşturma verisinin hazırlanması ayrıca nitelikli sertifikanın düzenlenmesi ve kaydedilmesinde § 18'in aradığı gereklere uygun teknik bileşen ve yöntemleri kullanmalıdır.

Sertifika hizmet sağlayıcısı imza oluşturma verisini yetkisiz müdahalelere karşı korumalıdır

Güvenli elektronik imza için, ihtiyari akreditasyon (md. 17) çerçevesinde, 1-3. fıkralardaki koşulların mevcut olduğunu belgelemelidir

Sertifika hizmet sağlayıcısı güvenli elektronik imza yöntemi sunuyorsa, güvenli bir elektronik imzanın sözkonusu olduğu hususunu sertifikada veya elektronik olarak her zaman ulaşılabilir olan bir listede belirtmek zorundadır

Mahkeme veya diğer kurumların talebi üzerine sertifika hizmet sağlayıcısı, kendi nitelikli sertifikasına istinad eden güvenli imzanın kontrolünü yapmak durumundadır.

Nitelikli Sertikanın tanzimi

§ 8 Sertifika hizmet sağlayıcı, nitelikli bir sertifika tanzim edilmesi gereken kişilerin kimliklerini, resmi, fotoğraflı bir kimlik belgesi vasıtasıyla güvenilir bir şekilde tespit etmek zorundadır. Sertifika hizmet sağlayıcı, belirli bir imza kontrol verisinin bu kişiye olan bağlantısını nitelikli bir sertifika ile tasdik etmek (teyit etmek, onaylamak) durumundadır.

Nitelikli bir sertifikanın tanzim edilmesi talebi, sertifika talep eden kişinin kimlik kontrolünü yapacak olan, sertifika hizmet sağlayıcının namına (adına) görev yapan diğer bir makama (kuruma) da yapılabilir.

Sertifika hizmet sağlayıcı sertifikalandırma taslağı çerçevesinde (na göre), sertifika sahibinin (talep eden kişinin) talebi üzerine kendi temsil yetkisi hakkında veya hukuken önemli diğer bir niteliğe ilişkin bilgilere nitelikli sertifika yer verilmesi konusunda, bu koşullar (hususlar, sebepler) kendisine veya diğer bir makama güvenilir bir şekilde ispatlandığında yer vermek durumundadır.

Sertifika hizmet sağlayıcısı sertifikalandırma konsepti çerçevesinde, sertifika sahibinin talebi üzerine sertifikada, imza sahibinin adı yerine takma adına da yer verebilir. Takma adın ne ahlaka aykırı olması ne de açıkça adlar veya rumuzlarla karışıklığa meydan vermeyecek nitelikte olması gerekir.

2. 5070 Sayılı Kanun md. 11: Nitelikli Elektronik Sertifikaların İptal Edilmesi = Avusturya İmza Kanunu md. 9

Sertifikaların İptali

§ 9 Sertifika hizmet sağlayıcısı bir sertifikayı eğer,

1. imza sahibi veya sertifikada anılan yetki sahibi kimse bunu talep ederse,
2. sertifika hizmet sağlayıcısı imza sahibinin öldüğünü veya bu tür sertifikada değişiklik yapılmasını gerektirecek sebeplerin ortaya çıktığını öğrenirse,
3. sertifikanın doğru olmayan bilgiler üzerine düzenlendiği anlaşılırsa,
4. sertifika hizmet sağlayıcı faaliyetini tatil ederse ve kendi listeleme ve iptal hizmetleri diğer bir sertifika hizmet sağlayıcı tarafından üstlenilmezse,
5. Denetim makamı md. 14'e göre sertifikanın iptali talimatı vermişse,
6. sertifikanın kötüye kullanılma tehlikesi mevcutsa,

gecikmeksizin iptal etmek zorundadır.

Fıkra 1'de anılan sebeplerin (durumların) kuşkuya yer vermeyecek şekilde derhal (gecikmeksizin) tespiti yapılamıyorsa, sertifika hizmet sağlayıcısı sertifikayı herhalukarda gecikmeksizin bloke etmek zorundadır

Blokaj ve iptal, geçerli oldukları anı (tarihi) ihtiva etmek zorundadır. İptal hizmeti veriliyorsa, blokaj ve iptal ilgili listeye kaydedildiği anda etkili olacaktır. Geriye yürürlü (etkili) bir blokaj ve iptal caiz değildir. İmza sahibi, özellikle halefi blokaj ve iptalden derhal haberdar edilmelidir.

Sertifika hizmet sağlayıcı bloke edilen veya iptal edilen nitelikli sertifikaların bir listesini elektronik olarak her zaman ulaşılabilir bir şekilde hazır bulundurmak zorundadır.

Denetim makamı bir sertifika hizmet sağlayıcısının sertifikasını, eğer

1. sertifika hizmet sağlayıcısnın faaliyetinin icrası yasaklanmışsa ve onun fihrist ve iptal hizmetleri başka bir sertifika hizmet sağlayıcı tarafından üstlenilmemişse; veya
2. sertifika hizmet sağlayıcısı faaliyetini tatil eder ve kendi fihrist ve iptal hizmetleri başka bir sertifika hizmet sağlayıcı tarafından üstlenilmemişse

derhal iptal edecektir.

3. 5070 Sayılı Kanun md. 8: Zaman damgası = Avusturya İmza Kanunu md. 10 =İmza Yönetmeliği md. 14

Zaman Damgası Hizmeti

§ 10 Sertifika hizmet sağlayıcı zaman damgası hizmeti veriyorsa, güvenlik ve sertifikalandırma taslağında bu konuda ayrıntılı bilgilere yer vermelidir. Güvenli zaman damgası hizmeti için, zaman bilgilerinin doğruluğunu ve gerçekliğini sağlayacak (güvence altına alacak) ve md. 18'de aranan şartları taşıyan teknik bileşenler ve yöntemler kullanılmalıdır.

Güvenli Zaman Damgası Hizmetleri (Yönetmelik Hükmü)

§ 14 Zaman damgası hizmetlerinin ifası için münhasıran nitelikli ve sadece bu amaç için düzenlenmiş olan sertifikaların kullanılması gerekir. Bu kullanım amacının sertifikada belirtilmesi gereklidir.

Tasdik edilen zaman bilgilerinin (tarih ve saat ayarı) yaz saati uygulaması da dikkate alınarak orta avrupa zaman dilimine uygun olması gerekir; diğer zaman dilimlerinin açıkça belirtilmesi gereklidir. Gerçek zaman biriminden söz konusu olabilecek bir sapmanın,

zaman damgası hizmeti sağlayıcısı nezdinde maksimum 1 dakika ile sınırlı olması gerekir (1 dakikayı aşmaması gerekir).

Güvenli zaman damgası hizmetlerinden yararlanılabilecek sürenin, bu hizmeti sunan sertifika hizmet sağlayıcısının güvenlik konseptinde belirtilmesi zorunludur.

4. 5070 Sayılı Kanun md. 10/g: Dokümantasyon (kayıt saklama) = Avusturya İmza Kanunu md. 11 = İmza Yönetmeliği md. 16

Dokümantasyon

§11 sertifika hizmet sağlayıcısı bu kanun ve bu kanuna istinaden çıkartılan yönetmeliğe riayet etmek amacıyla aldığı güvenlik tedbirlerini, ayrıca sertifikaların tanzimi ve gerekirse blokajı ve iptallerinin dokümantasyonunu yapmak zorundadır. Bu kapsamda veriler ve gerçeklikleri ayrıca bunların kayıt sistemine girildikleri tarihin her zaman kontrol edilebilir olması gerekir.

Mahkeme veya diğer makamların talepleri üzerine sertifika hizmet sağlayıcı dokümantasyonları fıkra 1'e göre teslim etmek durumundadır.

Belgeleme (Dokümantasyon)
(Yönetmelik Hükmü)

§ 16 Madde 11 SigG'ye göre yapılacak belgelemenin, arıza durumlarının ve özel işletim durumları ayrıca md. 20'ye göre sertifika sahibinin bilgilendirilmesi de dahil olmak üzere, her halükarda elektronik formda yapılması gereklidir. İmza oluşturma verilerinin oluşturulmasının imza sahibinin imza oluşturma ünitesi dışında gerçekleştiği hallerde, bu kural imza oluşturma verilerinin imza oluşturma ünitesine transferi anında da geçerlidir. Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcısının yaptığı dokümantasyonun

ihtiva ettiği verilerin sertifika hizmet sağlayıcının güvenli elektronik imzasıyla imzalanması ve güvenli bir zaman damgası ihtiva etmesi şarttır.
Birinci fıkraya göre yapılan belgelendirmelerin son tescilden (kayıttan) itibaren 33 yıl süre ile muhafaza edilmesi ve bu süre zarfında okunabilir ve erişilebilirliği sağlanmalıdır.

5. 5070 Sayılı Kanun md. 10/a: Personelin Nitelikleri = Avusturya İmza Yönetmeliği md. 10

Nitelikli Sertifikalar ve Güvenli Elektronik İmzalara İlişkin Sertifikalandırma ve İmza Hizmetlerinin Yerine Getirilmesi

§ 10 Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcısına ait donanımlar organizasyon veya teknik olarak ayrı yürütülüyorsa, bu durumda, alınacak güvenlik önlemleri sayesinde, alt bölümler arasında verilerin transfer edilmesinin imza veya sertifikalandırma hizmetlerinin tehlikeye maruz bırakılması sonucu doğurmayacağının güvence altına alınmış (garanti edilmiş) olması gerekir.

Bir sertifika hizmet sağlayıcısının teknik donanımlarının, sunulan imza ve sertifikalandırma hizmetlerine ilişkin olan fonksiyonları ve kullanımlarının diğer fonksiyon ve kullanımlardan ayrı olacak şekilde şekillendirilmiş (teşkil edilmiş olması) olması gereklidir. İmza ve sertifikalandırma hizmetlerinin diğer fonksiyon ve kullanımlardan etkilenmesi engellenmiş olmalıdır. Bu durumun hem normal iş süreci hem de özel işletim durumları ve i letim dışı (kullanım dışı) durumlarında da yerine getirilmesi (sağlanması) gerekir. Özel işletim durumlarının (örneğin; bakım) belgelenmesi gereklidir.

Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcı, imza ve sertifikalandırma hizmetlerinin yerine getirilmesi için gereken donanımlarını yetkisiz girişlere karşı koruyacak uygun tedbirler (önlemler) almak zorundadır.

Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcı, sunduğu imza ve sertifikalandırma hizmetleri kapsamında, kasden işlediği bir fiilden ötürü bir yıldan daha uzun süreli özgürlüğü kısıtlayıcı ceza (hapis cezası) almış veya mala karşı varlığına karşı işlediği veya belgelerin ve delillerin güvenilirliği aleyhine işlediği bir suçtan dolayı üç aydan daha uzun süreli hapis cezası almış kişileri çalıştıramaz. 1972 tarihli Adli Sicilden Silinme Kanununun hükümlerine göre silinmiş veya sadece sınırlı bir çerçevede hakkında bilgi edinilmesi mümkün olan mahkumiyet kararları gözönünde bulundurulmayacaktır. Personelin güvenilirliği sertifika hizmet sağlayıcı tarafından asgari iki yıllık aralıklarla kontrol edilmelidir.

Nitelikli sertifika tanzim eden bir sertifika hizmet sağlayıcısının teknik personeli, aşağıdaki branşlar hakkında yeterlii ölçüde uzman bilgiye (branş) sahip olmalıdır:

1. Genel EDV-Eğitimi
2. Güvenlik teknolojileri, kriptografi, elektronik imza ve Açık Anahtar Altyapısı (PKI)
3. Teknik, özellikle değerlendirme normları, ayrıca
4. Donanım ve yazılım.

Denetim makamının talebi üzerine, sertifika hizmet sağlayıcı tanınan eğitim kurumlarından alınan ilgili eğitimler veya ilgili branş faaliyetleri uyarınca çalıştırdığı personelin yeterli teknik bilgiye sahip olduğunu ispat etmek zorundadır. Münferit branşlara ilişkin olarak teknik personelin eğitiminin en az iki yıl sürmüş olması gerekir. Yeterli branş bilgisi örneğin; ilgili Yüksek Teknik Okul, bu tür bir meslek lisesi veya ilgili bir eğitim bitirilerek kazanılabilir. Bu eğitim ilgili branşta asgari üç yıl süren bir çalışma ile ikame edilebilir.

İmza oluşturma verileri sertifika hizmet sağlayıcıya ait yerlerde üretiliyorsa, bunların sadece imza sahibine verilmesi (teslim edilmesi) gerekir. İmza oluşturma verilerinin kullanımının imza sahibine teslim edilmesinden önce mümkün olması olanağının önlenmesi gerekir (bertaraf edilmesi gerekir). Her halukarda sertifika hizmet sağlayıcı, imza sahibinin imza

oluşturma verileri ve ilgili sertifikanın imza kontrol verilerinin tamamlayıcı şekilde kullanılabileceği konusunda tam kanaat uyandırmalıdır.

Sertifika hizmet sağlayıcı, imza sahibini imza oluşturma verilerinin ilk kullanımından önce, kullanım sırasında güvenlik açısından önemli olan tüm tedbirler hakkında (örneğin; yetkilendirme (tanımlama) kodlarının güvenliği, yabancı kullanımın hariç bırakılmasının kontrolü, fihrist ve iptal hizmetlerinin kullanılması, imzalanan verilerin görülmesi olanağı, uygun formatın kullanımı) yazılı veya sağlam (kalıcı) bir veri taşıyıcı kullanılmak kaydıyla açık ve genel olarak anlaşılabilir bir şekilde bilgilendirmek zorundadır.

6. 5070 Sayılı Kanun md. 11 Sertifika Hizmet Sağlayıcının Faaliyetinin Sona Ermesi= Avusturya İmza Kanunu md. 12

Faaliyete Son Verilmesi

§ 12 Sertifika hizmet sağlayıcısı faaliyetine son verdiğini gecikmeksizin Denetim makamına bildirmek zorundadır. Ayrıca sertifika hizmet sağlayıcısı faaliyetine son verdiği tarihte geçerli olan sertifikaları iptal etmek veya en azından fihrist ve iptal hizmetlerinin başka bir sertifika hizmet sağlayıcı tarafından üstlenilmesini sağlamaya çalışmak durumundadır. İmza sahibine faaliyete son verildiği, yine iptal veya devir keyfiyetleri derhal haber verilmelidir. Sertifikanın iptal edilmesi durumunda dahi sertifika hizmet sağlayıcısı, iptal hizmetlerinin devam ettirileceğini garanti etmek (sağlamak) zorundadır; bu yükümlülüğe uymazsa, denetim makamı iptal hizmetlerinin devamını masrafları sertifika hizmet sağlayıcısına ait olmak üzere sağlar.

7. 5070 Sayılı Kanun md. 6: Güvenli Elektronik İmza Oluşturma Araçları = Avusturya İmza Kanunu md. 18 = İmza Yönetmeliği md. 3 ve 4.

5. Bölüm

Teknik Güvenlik Kriterleri (Koşulları)

Güvenli İmza İçin teknik Bileşenler ve Yöntemler

§18 İmza oluşturma verilerinin hazırlanması ve kaydedilmesi ve ayrıca güvenli elektronik imzanın oluşturulması için, imzaların sahteliğini, bunun dışında imzalanan verilerin tahrif edilip edilmediğinin güvenilir bir şekilde fark edilmesini sağlayacak ve imza oluşturma verilerinin yetkisiz kullanımını güvenilir bir şekilde engelleyecek teknik bileşenler ve yöntemler kullanılacaktır.

Güvenli bir imzanın oluşturulması aşamasında kullanılan teknik bileşenler ve yöntemlerin bundan başka, imzalanan verilerin değiştirilemeyeceğini de garanti etmesi gerekir; bunların ayrıca imza sahibinin imzalanacak verileri imza atılmadan önce görmesini mümkün kılması gerekir. İmza oluşturma verileri sadece bir kez kullanılabilir, kopyalanamaz başkaları tarafından görülemezler ve bunların gizliliklerinin garanti edilmiş olması gerekir.

Nitelikli sertifikaların oluşturulması ve kaydedilmesinde, sertifikalarda sahtelik ve tahrifat yapılmasını engelleyecek bu tür teknik bileşen ve yöntemlerin kullanılması gerekir.

Güvenli imzalı verilerin kontrolünde,

1. imzalı verilerin değiştirilmemesini,
2. imzanın güvenilir şekilde kontrolünü ve bu denetimin sonuçlarını doğru (tam) olarak gösterecek
3. denetimi yapan kişinin elektronik imzanın hangi verilere ilişkin olduğunu tespit edebilmesini

4. kontrolü yapan kişinin elektronik imzanın hangi imza sahibine bağlı olduğunu tespit edebilmesini, takma adın
5. imzalanan verilerdeki güvenlik açısından önemli değişikliklerin farkedilebilmesini

sağlayacak (güvence altına alacak) nitelikte teknik bileşenler ve yöntemler kullanılacaktır.

Güvenli Elektronik İmza İçin İmza Oluşturma Verilerinin Hazırlanması (Yönetmelik hükmü)

§ 3 Denetim makamının imza oluşturma verilerinin EK I md. 1'e uygun olması gerekir (Ana sistem). İmza oluşturma sisteminin izole edilmiş olması, münhasıran bu amaç için tahsis edilmiş bir ortam olması ve her türlü dış müdahale ve çökmelere karşı uygun bir şekilde korunaklı olması gerekir. Denetim makamı kendi imza oluşturma verileri için, imza oluşturma verilerinin ikili bir sistemini oluşturmak (çift anahtar sistemi) ve kendi tuttuğu fihristleri imzalamak için kullanacağı kendine ait tüm elektronik imzaları, bu çift anahtar sistemi ile birlikte yedeklemek zorundadır. Çift anahtar sistemindeki imza kontrol verisi (açık anahtar) denetim makamının imza oluşturma verileriyle imzalanacaktır. Çift anahtarın güvenli bir şekilde saklanması gerekir. Çift anahtar sisteminin imza kontrol verileri sadece ana sistemin çökmesi durumunda kullanılabilecektir, ki bu durumda dahi denetim makamının imza ve sertifikalandırma hizmetlerinin sorunsuz şekilde işlerliği güvence altına alınmış olsun. Denetim makamı tarafından EK 1 md. 1'de sayılan imza oluşturma verilerinden başka bir imza oluşturma verisi kullanıldığında, ilgili imza kontrol verilerini ihtiva eden sertifikalar ana sistem tarafından imzalanmalı ve elektronik olarak her zaman erişilebilir olmalıdır. Denetim makamı kendisi tarafından kullanılan ilgili sertifikanın imza oluşturma verilerinin ve imza kontrol verilerinin tamamlayıcı şekilde kullanılabilir olmasını sağlamalıdır.

Sertifika hizmet sağlayıcısının imza oluşturma verileri kendisine ait imza oluşturma ünitesinde üretilmeli ve buradan asla dışarıya çıkartılmamalıdır. Oluşturulan imza kontrol verileri Sertifika Hizmet Sağlayıcının güvenlik ve sertifikalandırma konsepti içinde denetim makamına verilmelidir. Bunun dışındaki hallerde, diğer imzalayanlar için güvenli elektronik imza oluşturulması için aranan koşullar geçerli olacaktır.

İmza sahibinin güvenli elektronik imzası için gerekli olan imza oluşturma verileri, EK 1, md. 2'de tespit edilen asgari uzunlukta olmalıdır. Sertifika hizmet sağlayıcının güvenlik konseptinde kullandığı imza yönteminin gerçek anahtar uzunluğu alt ve üst sınır değerleri belirtilerek gösterilmelidir. Kullanılan algoritmaların açıklanmış olması gerekir. Güvenli elektronik imza için gerekli olan imza oluşturma verileri, mutlaka sadece imza sahibi tarafından görülebilmelidir. İmza oluşturma verilerinin tekniğin ulaştığı seviyeye göre, açıkça imza sahibinin kim olduğunun tespitini mümkün kılması gerekir. Güvenli elektronik imzalar için gerekli olan imza oluşturma verilerinin tekrar üretilmesi, kullanılan (ilgili) her bir imza yönteminin sahip olduğu güvenlik seviyesine göre anahtar kalitesinin azalmasına kesinlikle yol açmamalıdır.

Güvenli elektronik imzalar için gerekli olan imza oluşturma verilerinin tekrar kullanımı anahtar kalitesinin düşmesine yol açmamalıdır. İmza oluşturma verilerinin kalitesini azaltabilecek kullanımlar (örneğin; tesadüfen seçilen veriler için RSA kullanımları) etkin bir şekilde bertaraf edilmelidir. İmza oluşturma verileri sadece tespit olunan amaç için kullanılabilecektir.

Güvenli elektronik imzalar için gerekli olan imza oluşturma verilerinin oluşturulması, gereçk bir olasılığa dayanmaktadır. Bu olasılığın temelinde ya teknik ya da imza sahibine ilişkin bir olasılık mevcuttur. İmza oluşturma verilerinin Ek 1 md. 3'de tespit edilen bit dizgisi sayılarının gerçek tesadüf elementleri (unsurları) tarafından (etkilenmiş olması şarttır). Tesadüf unsurlarının uygunluk açısından yeteri ölçüde denetlenmiş olması şarttır. Takma (Pseudo) tesadüf rakamları başlangıç (çıkış) esası olarak kullanılmayacaktır. Oluşturma sistemi, farklı imza sahiplerinin imza oluşturma verileri bakımından kullanılmışsa, kullanılan teknik olasılığın periyodik olarak, en azından bir aylık aralıklarla istatistiki tesadüf kalitesi kontrol edilmelidir. Kontrol proteokolleri belgelenmelidir. Olumsuz bir kontrol sonucu ortaya çıkarsa, ilgili imza oluşturma verilerine dayanan ve son yapılan kontrolde elde edilen olumlu sonuç üzerine tanzim edilmiş olan sertifikalar iptal edilecektir.

Güvenli elektronik imzalar için gereken imza oluşturma verilerinin sertifika hizmet sağlayıcılara ait yerlerde üretilmesi durumunda, sertifika hizmet sağlayıcı bu imza oluşturma

verilerinin veya imza oluşturma verileri hakkında kendilerinden bilgi edinilebilecek diğer verilerin öğrenilmesini, ayrıca bu verilerin imza sahibinin imza oluşturma ünitesi dışında kaydedilmesini önleyecek tedbirler almalıdır. Bu kural aynı zamanda bu tür imza oluşturma verilerinin imza sahibinin, imza oluşturma ünitesine transferi ve ayrıca imza sahibinin imza oluşturma ünitesi karşısında tespitini (tespit edilmesini) sağlayan veriler hakkında da uygulanacaktır (örneğin; PIN). İmza oluşturma verilerinin hazırlanması, imza sahibinin imza oluşturma ünitesi dışında gerçekleştirilecekse, bu durumda dışarıdan gelebilecek her türlü müdahale ve tehditlere karşı koruma sağlayacak bir oluşturma sisteminin kullanılması gerekir. Oluşturma verisinin kullanımı gözlenmeli, her kullanıcı teşhis edilmeli (tespit edilmeli) ve her kullanım kaydedilmelidir.

Güvenli elektronik imzalar için gereken imza oluşturma verileri, imza sahibinin imza oluşturma ünitesinde üretilmişse, bu durumda sertifika hizmet sağlayıcı imza oluşturma verilerinin hem oluşturulması hem de kaydedilmesi için sadece teknik açıdan uygun olan imza oluşturma ünitelerini sunmalı veya tavsiye etmelidir.

Güvenli elektronik imzalar için gerekli olan imza oluşturma verilerinin kaydedilmesi (Yönetmelik Hükmü)

§ 4 Güvenli elektronik imza için gereken imza oluşturma verileri, başkaları tarafından öğrenilmelerini engelleyecek ve kullanımları ancak imza sahibinin münhasır kontrolünde olacak şekilde kaydedilmelidir. İmza oluşturma verilerinin oluşturulduktan sonra çoğaltılması caiz değildir.

Özel güvenlik amaçlarıyla güvenli elektronik imzalar için gereken imza oluşturma verileri birden çok imza oluşturma ünitesine dağıtılabilir. Bu durumda güvenlik kriterlerinin ilgili imza oluşturma ünitelerinin hepsi tarafından yerine getiirlmesi gerekir. İmza sahibi imza fonksiyonun çözülmesi için gereken tedbirler hakkında bilgilendirilmelidir.

8. 5070 Sayılı Kanun md. 10/e, f: Bilgilendirme Yükümlülüğü = Avusturya İmza Kanunu md. 20, 21

6. Bölüm

Kullanıcının Hakları ve Yükümlülükleri

Sertifika Hizmet sağlayıcının Genel Bilgilendirme Yükümlülüğü

§ 20 Sertifika hizmet sağlayıcısı sertifika talep sahibini, sözleşmenin aktedilmesinden önce yazılı olarak veya kalıcı bir veri taşıyıcı kullanarak açık ve genel olarak anlaşılır bir biçimde güvenlik ve sertifikalandırma konseptinin içeriği hakkında bilgilendirmek zorundadır. Nitelikli bir sertifikanın düzenlenmesi durumunda, sertifika hizmet sağlayıcısı ayrıca (bundan başka) sertifikanın kullanım şartları örneğin; kullanım alanına ilişkin veya işlem değerine ilişkin sınırlamaları bildirmek; bunun dışında ihtiyari akreditasyon ve yine özel uyuşmazlık çözüm yöntemlerine dikkat çekmek zorundadır.

Talep üzerine 1. fıkrada sayılan bilgiler, bu konuda hukuki menfaat sahibi olduğu yolunda kanaat uyandıran üçüncü kişiler için de açık (erişilebilir) tutulabilir.
Bir sertifika hizmet sağlayıcısı ayrıca sertifika sahibini, kullanılan imza yöntemi bakımından hangi teknik bileşenlerin ve yöntemlerin uygun olduğu konusunda ve gerekirse güvenli imzanın oluşturulması ve kontrolü için istenilen koşulların yerine getirilmesi için hangi teknik bileşenlerin ve yöntemlerin ve sair tedbirlerin alınması gerektiği konusunda da bilgilendirmelidir. Ayrıca sertifika sahibini kullandığı imza yönteminin olası hukuki sonuçları hakkında, imza sahibinin yükümlülükleri ve ayrıca sertifika hizmet sağlayıcının özel sorumluluğu hakkında aydınlatmalıdır. Sertifika hizmet sağlayıcı sertifika sahibi ayrıca mevcut imzanın güvenlik değeri zamanla azalacağı için, gerekirse ve herhalükarda nasıl yeni bir elektronik imza düzenleyeceği konusunda da bilgilendirir.

İmza Sahibinin Yükümlülükleri

§21 İmza sahibi imza oluşturma verilerini özenli (dikkatli) bir şekilde saklamak, ayrıca imza oluşturma verilerine yapılabilecek öngörülebilir saldırıları (tecavüzleri) engellemek ve başkalarına vermemekle yükümlüdür. İmza oluşturma verisi kaybolmuşsa, imza oluşturma verisinin tehlikeye maruz kalması tehlikesi mevcutsa veya sertifikada belirtilen şartlar değişmişse, imza sahibi sertifikanın iptalini talep edebilecektir.

9. 5070 Sayılı Kanun md. 14: Yabancı Sertifikalar = Avusturya İmza Kanunu md. 24

7.Bölüm
Yabancı Sertifikaların Tanınması
Tanıma

§ 24 Avrupa Topluluğunda yerleşik bir sertifika hizmet sağlayıcı tarafından tanzim edilen ve geçerlilikleri ülke dışında kontrol edilebilecek olan sertifikalar, yerli (ülke içindeki) sertifikalarla eşdeğerlidir. Bu sertifika hizmet sağlayıcılarının nitelikli sertifikaları, ülke içindeki (yerli) nitelikli sertifiklarla aynı hukuki sonuçlara sahiptir.

Üçüncü bir ülkede yerleşik bir sertifika hizmet sağlayıcı tarafından hazırlanan ve geçerlilikleri ülke dışında kontrol edilebilen sertifikalar, ülke içinde tanınacaktır. Nitelikli sertifikalar, aşağıdaki şu durumlarda ülke içindeki nitelikli sertifikalarla hukuki açıdan eşdeğerli olarak kabul edilecektir:

1. sertifika hizmet sağlayıcı md. 7'nin aradığı şartları yerine getirmişse ve Avrupa Birliğine üye bir devletin ihtiyari akreditasyon sistemi içinde kendini akredite ettirmişse,
2. Madde 7'de aranan koşulları yerine getiren Avrupa Topluluğu içinde yerleşik bir sertifika hizmet sağlayıcı, sertifika için sorumluluk hukuku anlamında garanti verirse veya
3. bir taraftan Avrupa topluluğu ve öte taraftan üçüncü devletler veya uluslararası organizasyonlar arasındaki iki veya çok taraflı anlaşmalar çerçevesinde, sertifika nitelikli sertifika veya sertifika hizmet sağlayıcı nitelikli sertifika tanzim eden olarak tanınmışsa.

Avrupa Birliğine üye bir devlette veya bir üçüncü ülkede güvenli elektronik imza için aranılan güvenlik kriterleri (koşulları) ispat amacıyla resmi olarak tanınan bir makama ibraz edildiğinde, denetim makamı, bu makamın mütalaalarına esas teşkil eden teknik koşulların, kontrollerin ve kontrol yöntemlerinin her birinin tasdik makamının ki ile eşdeğerli olduğunu tespit ettiği durumda, bu makamın verdiği güvenli elektronik imza oluşturulması konusundaki güvenlik kriterlerine riayet edilmesine ilişkin belgeler, tasdik makamının vesikaları ile eşdeğerli olarak kabul edilecektir.

10. 5070 Sayılı Kanun md. 11/f.2: Sertifika İptal Listeleri (fihrist) = Avusturya İmza Yönetmeliği md. 13

Nitelikli Sertifikalar İçin Fihrist ve İptal Hizmetleri

§ 13 Fihrist ve iptal hizmetleri için format olarak, özellikle EK 2 md. 6'da anılan format uygundur. Fihrist ve iptal hizmetlerinin farklı formatlarda hazırlanması (sunulması) da mümkündür. Sertifika hizmet sağlayıcı, iptal hizmetlerinin formatının denetim makamı tarafından yürütülmesi (devam ettirlmesi) açısından uygun olduğunu garanti etmelidir. Fihrist ve iptal hizmetleri diğer bir sertifika hizmet sağlayıcı tarafından üstlenilmişse, bu duurmda bu sertifika hizmet sağlayıcının da aynı formatta hizmet vermesi gerekecektir.

Sertifika hizmet sağlayıcı, imza sahibi ve ayrıca üçüncü kişiye, imza sahibinin temsil yetkisi hakkındaki bilgileri nitelikli bir sertifi içine dahil etmek, sertifikanın her zaman gecikmeksizin sağlayacak uygun iletişim bilgilerini bildirmek durumundadır.

Fihrist ve iptal hizmetleri sahtecilik, tahrifat ve yetkisiz taleplere karşı korumalı olmalıdır. Sadece yetkili kişilerin fihristlerde kayıt veya değişiklik yapması sağlanmış olmalıdır. Ayrıca bir blokajın veya iptalin farkedilmeksizin geri alınmasının mümkün olmaması, temin edilmelidir.

İptal hizmetlerinin güncellenmesi iş saatleri sırasında (iş saatleri içinde) en geç iptal sebebinin bildirilmesinden itibaren üç saat zarfında gerçekleştirilmelidir. İş saatlerinin iş günleri içinde en azından saat 9:00'dan 17:00'ye kadar olan zamanı e Cumartesi günleri için saat 9:00'dan 12:00'ye kadar olan zamanı kapsaması gerekir. İş saatleri dışında sertifika hizmet sağlayıcının, nitelikli bir sertifikanın iptali talebini her zaman otomatik olarak alacak ve blokajı gerçekleştirecek bir sistem kurması gerekir.

Fihrist hizmetlerinden istifade edilebilecek olan sürenin (zaman diliminin) güvenlik konseptinde belirtilmiş olması gerekir. Fihrist hizmetlerinin en azından md. 4'teki iş saatleri süresince erişilebilir olması gerekir. İptal hizmetlerinin daimi olarak erişilebilir olması zorunludur (hazır olması). Fihrist ve iptal hizmetlerinin kullanılabilecekleri zaman zarfında 30 dakikadan daha fazla kesintisiz olarak sekteye uğraması, arıza durumları olarak belgelendirilmelidir. İptal hizmetlerinin bakımı ve arıza durumları için, yedek bir sistemin hazır bulundurulması gerekir. Yedek sistemin de devre dışı kalması durumunda, bu durumun bir takvim günü zarfında denetim makamına bildirilmesi gerekecektir. Denetim makamı üç takvim günü zarfında iptal hizmetini tekrar eski haline getirecektir. İptal hizmetleri genel

olarak serbestçe erişilebilir olmalıdır. İptal hizmetlerinin soruşturulması ücretsiz ve kimlik tespiti yapılmadan mümkün olmalıdır.

Bir sertifika hizmet sağlayıcının fihrist ve iptal hizmetlerini en azından yeniden imza oluşturmanın (nachsignieren) gerekeceği zamana kadar sürdürmesi gerekir. Bu sürenin geçmesinden sonra sertifika hizmet sağlayıcının, somut olayda nitelikli sertifikanın kontrolünü md. 16/f.2'de anılan sürenin sona ermesine kadar mümkün olması gerekir. Aynı durum bir sertifika hizmet sağlayıcısının faaliyetine son vermesi veya faaliyetinin yasaklanması durumunda denetim makamı tarafından iptal hizmetlerinin yürütülmesi bakımından da geçerlidir.

Bir blokajın etkili olabileceği zaman süresinin güvenlik konseptinde belirtilmiş olması zorunludur. Bu sürenin üç iş gününü aşmaması gerekir. Bu süre zarfında bir blokajın kaldırılması mümkündür. Kaldırılan bir blokajın sertifikanın geçerliliği üzerinde etkisi yoktur. Belirtilen süre zarfında blokaj kaldırılmamışsa, sertifika iptal edilecektir. Bir blokaja istinaden bir sertifikanın iptali gerçekleştirilirse, evvelce yapılan blokaj iptal olarak geçerli olacaktır.

İmza sahibinin imza oluşturma verisi öğrenilirse veya bu, imza sahibinden başka (imza sahibinin dışında) imza oluşturma verileri olarak veya diğer bir şekilde vuku bulursa, bu durumda imza sahibinin sertifikasının iptalini gerektirecek şekilde imza oluşturma verilerinin tehlikeye maruz bırakılması söz konusu olacaktır. İptalin imza sahibi tarafından talep edilmesi (md. 9/f.1 b.1 SigG) veya bu durum hakkında bilgi sahibi olur olmaz sertifika hizmet sağlayıcının kendiliğinden bu iptal işlemini gerçekleştirmesi gerekecektir (md. 9/f. 1 b. 6 SigG).

11. 5070 Sayılı Kanun md. 8/f.2 (a,b,c): Güvenlik ve Sertifikalandırma Taslağı = Avusturya İmza Yönetmeliği md. 15

Nitelikli Sertifikalar İçin Güvenlik ve Sertifikalandırma Taslağı

§ 15 Güvenlik ve sertifikalandırma taslağının özellikle aşağıdaki şu içeriğe sahip olması gerekir:

1. Sertifika hizmet sağlayıcının adı
2. sertifika hizmet sağlayıcının adresi ve yerleşik olduğu ülke
3. Sunulan imza ve sertifikalandırma hizmetlerinin çeşidi, kullanım alanı ve yerine getirilmesi
4. talepte bulunma usulü
5. gerekirse sertifikada imza sahibinin takma adının yazılmasının tarzı ve şekli ayrıca yine imza sahibinin temsil yetkisi veya hukuken önemli sair (diğer) nitelikleri (özellikleri) hakkındaki bilgilere sertifikada yer verilmesinin tarzı ve şekli
6. çalışma saatleri
7. sertifika hizmet sağlayıcısının imza oluşturma verilerinin hazırlanması (oluşturulması)
8. sertifika hizmet sağlayıcının imza oluşturma verilerinin formatı
9. imza kontrol verileri, gerekirse sertifika hizmet sağlayıcının sertifikası
10. imza sahibinin imza oluşturma verilerinin oluşturulması
11. imza sahibinin imza oluşturma verilerinin formatı
12. sunulan imzanın hazırlanmasında (oluşturulmasında) kullanılan yöntemler (hash yöntemleri ve hash değerinin şifrelenmesi için kullanılan yöntemler)
13. Kullanılan, sunulan ve tavsiye edilen imza ürünlerinin listesi
14. yetkilendirme kodlarının güvenliği
15. imzalanan dokümanlar için kullanılabilir (kullanıllı, partik) formatlar ve gerekirse dinamik değişiklikleri önlemeye yarayacak yöntemler
16. sertifikaların formatları ve geçerlilik süreleri
17. blokaj süresi de dahil olmak üzere, sunulan fihrist ve iptal hizmetleri için teknik normlar, giriş yöntemleri ayrıca güncelleme ve hizmet süresi
18. icabı halinde sunulan zaman damgası hizmetleri için hizmet süresi
19. güvenli imza kontrolü için etkin ve genel olarak anlaşılabilir (açık) yöntemler
20. güvenlik tedbirlerinin, arıza durumlarının ve özel işletim durumlarının belgelendirilme formatı

21. Sertifikaların yeniden imzalanması (nachsignieren) süresi ve yöntemi
22. yetkisiz girişlere karşı sertfika hizmet sağlayıcısına ait donanımların korunmasına ilişkin önlemler

Güvenlik ve sertifikalandırma taslağının denetim makamına RTF, PDF, Ascii veya Postscript formatında elektronik formda ibraz edilmesi gereklidir. Bu taslağın sertifika hizmet sağlayıcısının güvenli elektronik imzasıyla imzalanması gerekir. Sertifika hizmet sağlayıcısı güvenlik ve sertifikalandırma taslağını ayrıca bir özeti genel olarak anlaşılması mümkün RTF, PDF, Ascii veya Postscript formatında elektronik olarak her zaman ulaşılabilir bir şekilde hazır bulundurmalıdır.

12. 5070 Sayılı Kanun md. 10/b,c (Kimlik Tespiti, Temsil Yetkisi) = Avusturya İmza Yönetmeliği md. 11

Nitelikli Bir Sertifika Tanzim Edilmesi Talebi

§ 11 Sertifika hizmet sağlayıcı sertifika talep eden kişinin kimliğini geçerli resmi fotoğraflı bir kimlik belgesine istinaden tespit etmelidir. Nitelikli bir sertifika tanzim edilmesi talebinin sertifika talep eden kişi tarafından el yazısı ile imzalanması zorunludur. İbraz edilen fotoğraflı kimlik belgesinden, taleple birlikte belgelendirilmek üzere bir örneğin hazırlanması gerekir. Bu tür talebin, sertifika talep eden kişinin kimliğinin tekrar tespitini önlemek amacıyla, sertifika talep eden kişinin güvenli elektronik imzasıyla imzalanması gerekir.

Nitelikli bir sertifika tanzim edilmesi talebinin özellikle şu hususları içermesi gerekir:

1. Sertifika sahibinin adı, doğum yeri ve tarihi ve ayrıca adresi, ibraz edilen fotoğraflı kimlik belgesinin tanzim tarihi ve numarası, ayrıca bu belgeyi düzenleyen makam.

2. gerekirse sertifikanın kullanım alanına ilişkin bir sınırlama veya işlem değerine ilişkin bir sınırlama ihtiva edip etmemesine yönelik bilgiler
3. gerekirse üçüncü kişiler için temsil yetkisi, sertifika talep eden kişinin hukuken önemli diğer nitelikleri örneğin; mesleki veya diğer izinler veya nitelikli sertifikada yer verilmesi gereken diğer bilgiler.

Nitelikli bir sertifikada üçüncü bir kişinin temsil yetkisi hakkında bilgilere yer verilmesi gerekiyorsa, temsil yetkisinin güvenilir bir şekilde ispatlanması ve yazılı veya güvenli bir elektronik imza ile imzalanmış bir şekilde üçüncü kişinin rızasının ibraz edilmesi gereklidir. Bu üçüncü kişi nitelikli sertifikanın içeriği hakkında yazılı olarak veya kalıcı bir veri taşıyıcı kullanılarak bilgilendirilmeli ve İmza kanunu md. 9/f.1, b.1'e (SigG) göre söz konusu olabilecek iptal olanağına dikkat çekilmelidir. Mesleki veya diğer sair bir iznin nitelikli bir sertifikaya kaydedilmesinden önce aynı şekilde güvenilir olarak ispatlanması gerekir. İmza sahibi kaydedilen mesleki nitelikleri bakımından kamu hukukuna ait bir meslek kontrolüne (denetimine) tabi ise, bu durumda mesleki denetimi yapan kurumun, nitelikli sertifikanın içeriği hakkında yazılı olarak veya kalıcı bir veri taşıyıcı kullanılarak bilgilendirilmesi gereklidir.

İSVEÇ NİTELİKLİ ELEKTRONİK İMZA KANUNU (SFS 2000:832)

1. 5070 Sayılı Kanun md. 6: Güvenli Elektronik İmza Oluşturma Araçları = İsveç İmza Kanunu md. 3

Güvenli İmza Yaratan Araçlar

Madde 3- Güvenli olduğu açıklanan bir imza yaratan araç, imzanın sahteciliğe karşı yeterince korunmasını sağlamak zorundadır. Araç, bundan başka imza yaratan datanın;

1. Usulüne uygun olarak sadece bir kere meydana gelebildiğini,
2. Elverişli araçlarla çoğaltılamadığını,

3. Yasal imzacı tarafından, başkalarının kullanımına ya da çoğaltmasına karşı yeterince korunmasını sağlamak zorundadır.

Güvenli imza yaratan araç, elektronik olarak imzalı bir datayı değiştiremez ya da imza sürecinden daha önce imzacıya, datanın sunulmasını önleyemez.

2. 5070 Sayılı İmza Kanunu md. 8: Elektronik Sertifika Hizmet Sağlayıcısı = İsveç İmza Yasası md. 9

Madde 9- Halka nitelikli sertifika yayınlayan bir sertifika sağlayıcı güvenilir davranışla faaliyetlerini idare edecektir ve

1. Uzman bilgiye ve özellikle yönetim, teknoloji ve güvenlik faaliyetleri için istenilen deneyime sahip personel çalıştıracaktır.
2. Kabul edilen standartlara uyan idare ve yönetim usulleri kullanacaktır.
3. Değişikliğe karşı korunan ve teknik ve kriptografik güvenlik sağlayan emniyetli sistem ve ürünler kullanacaklar.
4. Bu Kanunda yer alan şartlara göre işi idare edecek ve zararı taahhüt riskini üstlenecek yeterli finansal kaynakları koruyacaktır.
5. Nitelikli sertifikaları yayınlanan imzacıların kimliklerini doğrulayacak güvenlik usullerine sahip olacak.
6. Hızlı ve güvenli bir kayıt sistemini ve nitelikli sertifikaların derhal iptali sistemini koruyacaktır.
7. Nitelikli sertifika sahtekarlığına karşı önlemler alacak ve imza yaratan datanın üretimi aşamasında tamamen gizliliği uygulayabileceğini garanti edecektir.

1. cümlenin 3 nolu bendinde bahsedilen şartların, Avrupa Topluluğu Komisyonu tarafından kabul edilen ve Avrupa Topluluğunun Resmi Gazetesinde yayınlanan elektronik imza ürünlerinin standartları hakkındaki kaynak hükümlere uyan donanım ya da yazılım araçları tarafından yerine getirileceği kabul edilecektir.

3.5070 Sayılı İmza Kanunu md. 10: Sertifika Hizmet sağlayıcının Yükümlülükleri = İsveç İmza Kanunu md. 10

Madde 10- Halka nitelikli sertifika yayınlayan bir sertifika sağlayıcı:

1. İmzacıdan gelen bir talep halinde ya da bunu yapması gereken başka bir nedenin varlığı halinde derhal sertifikayı iptal edecek.
2. Sertifikanın yayınladığı ya da iptal edildiğinde, tarihin ve saatin tam olarak belirlenebilir olmasını sağlayacak.
3. Sertifika sağlayıcı tarafından, imza yaratan data ve imzanın doğruluğunu kanıtlayan datanın uyumlu olacak biçimde üretilmesi sağlanacak.

4. 5070 Sayılı Kanun md. 10/g: Dokümantasyon (kayıt saklama) = İsveç İmza Kanunu md. 11

Madde 11- Halka nitelikli sertifika yayınlayan bir sertifika sağlayıcı sertifikalarla ilgili tüm konularda makul bir süre için, sertifikanın tipine ve diğer şartlarına göre değişen bir kayıt tutmak zorundadır. Sertifika sağlayıcı ayrıca nitelikli sertifikaları doğruluğu kanıtlanabilir biçimde saklamak için emniyetli sistem kullanmak zorundadır. Onun için;

1. Sadece yetkili kişiler ekleme ve değişiklik yapabilir.
2. Bilginin hakikiliği kanıtlanabilir olmalıdır.
3. Sadece sertifika sahibinin rızası ile sertifikalar inceleyip doğruluğunu saptamak için alenen kullanılabilir ve
4. Bu güvenlik koşullarını tehlikeye maruz bırakabilecek herhangi bir teknik değişiklik operatörce kolayca saptanabilir.

Sertifika sağlayıcı imza yaratan datayı saklayamaz ya da kopyalayamaz.

5. 5070 Sayılı Kanun md. 10/e, f: Bilgilendirme Yükümlülüğü = İsveç İmza Kanunu md. 12

Madde 12- Sertifika sağlayıcı nitelikli bir sertifika çıkarılmasına dair bir sözleşme yapmadan önce, sertifika isteyen tarafı aşağıdaki konularda yazılı ve rahat anlaşılabilir bir dilde bilgilendirilir.

1. Serifikanın kullanılması ile ilgili sınırlamalar ve diğer şartlar.
2. Teknik Uygunluk Değerlendirme Kanunu (1992:1119) gereğince gönüllü bir kredilendirme ya da sertifikalandırma projesinin varlığı ve
3. Şikayetleri ve anlaşmazlıkları çözüme bağlama usulü.

Birinci bentte gösterilen bilgi elektronik olarak gönderilebilir.

Sertifikaya bağlı olarak, diğerleri de istenildiği zaman bilgiyi elde edebilirler.

6. 5070 Sayılı Kanun md. 11: Faaliyete son verme = İsveç İmza Yasası md. 20

Madde 20- Deneçi makam, bu Kanun ve bu Kanuna uygun olarak çıkarılan yöntmeliklere uygunluğu temin edebilmek için tedbir ve yasaklama kararları yayınlayabilir.

Denetçi makam, halka nitelikli sertifika yayınlayan ve nitelikli olduğunu onlara beyan eden bir sertifika sağlayıcıdan beklenen etkinlik düzeyine ulaşmadığı taktirde faaliyetlerini tamamen veya kısmen faaliyetini durdurmasını isteyebilir.

İSVİÇRE SERTİFİKA HİZMETLERİ TÜZÜĞÜ

1. 5070 Sayılı Kanun md. 10/b, c: Kimlik Tespiti = İsviçre İmza Tüzüğü md. 8

Madde 8: Elektronik Sertifika Verilmesi

Akredite edilmiş sertifika hizmeti sağlayıcıları, elektronik sertifika verilmesi talebinde bulunan kişilerden, aşağıdaki belgeleri bizzat ibraz etmek suretiyle kimliklerini ve temsil yetkilerini belgelemelerini isteyecektir:

a. Gerçek kişilerde kimlik cüzdanı veya pasaport;
b. İdarî birimler adına hareket edenlerden vekâletname ve kimlik cüzdanı veya pasaport;
c. Tüzel kişilerde ticarî mümessillerle ilgili ticaret sicili kaydı örneği ve kimlik cüzdanı veya pasaport.

On yıldan daha kısa bir süre önce 1. fıkra uyarınca kimliği belgelenmiş bir kişi veya idarî birim yeni bir elektronik sertifika talebinde bulunduğu takdirde, akredite edilmiş sertifika hizmeti sağlayıcıları özel anahtarla üretilmiş dijital bir imza taşıyan bir talebi kabul edebilirler, yeter ki özel anahtar sertifikası yenilenmek istenen kamuya açık anahtarla irtibatlandırılabilsin.

Sağlayıcılar, talep üzerine elektronik sertifikada onaylanmış kamuya açık anahtarın sahibinin adı yerine bir müstear ad gösterebilirler. Kimlik tespitinin 1. ve 2. fıkralar uyarınca yapılması zorunludur.

2. 5070 Sayılı Kanun md. 10/e, f: Bilgilendirme Yükümlülüğü = İsviçre İmza Tüzüğü md. 9

Madde 9: Bilgi Verme Yükümü

Sertifika hizmeti sağlayıcıları, kamunun genel sözleşme şartlarına ve sertifikasyon politikalarını ilişkin bilgilere ulaşabilmesini temin etmekle yükümlüdür.

Sertifika hizmeti sağlayıcıları, en geç elektronik sertifikaların verildiği tarihte, müşterilerini özel anahtarın kötüye kullanılması veya kaybedilmesinin sonuçları hususunda uyarmak

zorundadırlar. Onlara, özel anahtarın gizli tutulmasına yarayacak tedbirler önermeğe mecburdurlar.

3. 5070 Sayılı Kanun md. 11: Sertifikaların iptali = İsviçre İmza Tüzüğü md. 11

Madde 11: Elektronik Sertifikaların İptali

Akredite edilmiş sertifika hizmeti sağlayıcıları sahiplerinin talebi üzerine elektronik sertifikaları gecikmesizin iptal ederler.

Sağlayıcıların iptal talebinde bulunan kişinin bu hususta yetkili olduğuna kanaat getirmelere gerekir. Talepte, sertifikası iptal edilecek kamuya açık anahtarla irtibatlandırılan özel anahtarla atılan bir dijital imza bulunuyorsa, bu şart gerçekleşmiş sayılır.

Sertifika hizmeti sağlayıcıları, vermiş oldukları elektronik sertifikaların haksız ele geçirildiklerinin veya kamuya açık bir anahtarın belirli bir kişi veya idarî birimle irtibatlandırılması hususunda güven vermediklerinin anlaşılması halinde, o elektrik sertifikaları gecikmeksizin iptal etmekle yükümlüdürler.

Sağlayıcılar elektronik sertifikaları geçici olarak en çok üç gün süreyle askıya alabilirler. Bu sürenin bitiminde sertifikaları kesin olarak iptal eder veya yeniden geçerli sayarlar. Birinci şıkta, iptal askıya alma tarihinden itibaren hüküm ifade eder, ikinci şıkta, askıya alma sertifikanın geçerliliğine etki yapmaz.

Akredite edilmiş sertifika hizmeti sağlayıcıları elektronik sertifika sahiplerini bunların iptali veya askıya alınma durumundan gecikmeksizin haberdar ederler.

4. 5070 Sayılı Kanun md. 11/f. 2: Sertifika iptal listesi = İsviçre İmza Tüzüğü md. 12

Madde 12: Elektronik Sertifika Sicili ve İptal Edilen veya Askıya Alınan Sertifika Listeleri

Akredite edilmiş sertifika hizmeti sağlayıcıları, vermiş oldukları elektronik sertifikalar için, müşterilerin elektronik sertifikalarını kaydettirebilecekleri bir sicil tutarlar.

Sertifika hizmeti sağlayıcıları iptal ettikleri veya askıya aldıkları bütün sertifikalarında, sicile kaydedilmiş olmasalar bile, listesini tutmakla yükümlüdür. Bu listede münhasıran elektronik sertifikanın seri numarası; iptal edilmiş veya askıya alınmış olduğu, iptal veya askıya alınma tarihi ve saati belirtilir. Liste akredite edilmiş sertifika hizmeti sağlayıcısının dijital imzasıyla doğrulanır.

Sağlayıcılar üçüncü kişilere her zaman ve –kamusal telekomünikasyon araçlarından yararlanmanın giderleri dışında- ilâve hiçbir gider gerekmeksizin elektronik sertifika siciline ve iptal edilmiş ya da askıya alınmış sertifika listesine on-line girmek imkânını temin etmekle yükümlüdürler.

Elektronik sertifika sicillerinin ve iptal edilmiş veya askıya alınmış sertifika listelerinin nasıl tutulacağı, sicil ve listelere nasıl girileceği yönetmeliklerle düzenlenir.

5. <u>5070 Sayılı Kanun md. 11/g: Dokümantasyon = İsviçre İmza Tüzüğü md. 13</u>

Madde 13: Elektronik Sertifikaların Saklanması

Akredite edilmiş sertifika hizmeti sağlayıcıları süresi dolmuş veya iptal edilmiş elektronik sertifikalarla iptal edilmiş sertifika listelerini saklamak ve sertifika süresinin bitimi veya iptal tarihinden itibaren en az on bir yıl süreyle sertifikaların ve listelerin incelenmesi imkanını temin emekle yükümlüdürler.

İlk altı yılda söz konusu inceleme her zaman ve –kamusal telekomünikasyon araçlarından yararlanma giderleri dışında- başkaca hiçbir gider gerektirmeksizin online yapılabilecektir.

6. 5070 Sayılı Kanun md. 11: Faaliyete Son Verme = İsviçre İmza Tüzüğü md. 15

Madde 15: Faaliyete Son Verilmesi

Akredite edilmiş sertifika hizmeti sağlayıcıları SAS'a faaliyetlerini durdurduklarını 30 gün önceden bildirirler. Kendilerine yönelik bir iflas tehdidi SAS'a gecikmeksizin bildirilecektir.

Faaliyetlerini kendi istekleriyle durduran akredite edilmiş sertifika hizmeti sağlayıcıları vermiş oldukları, geçerliliğini koruyan elektronik sertifikaları iptal etmekle yükümlüdürler. SAS bir başka akredite edilmiş sertifika hizmeti sağlayıcısını iptal edilmiş sertifikaların listesini tutmak ve süresi dolmuş veya iptal edilmiş sertifikaları, faaliyet jurnali ile ilgili belgeleri saklamakla görevlendirir.

Akredite edilmiş bir sertifika hizmeti sağlayıcısı iflâs ettiği takdirde, SAS başka bir akredite edilmiş sertifika hizmeti sağlayıcısını iflas eden sağlayıcının vermiş olduğu, geçerliliğini koruyan elektronik sertifikaları iptal etmek, iptal edilmiş sertifikaların listesini tutmak ve süresi dolmuş veya iptal edilmiş sertifikalarla faaliyet jurnalini ve ilgili belgeleri saklamakla görevlendirir.

7. 5070 Sayılı Kanun md. 14: Yabancı Sertifikalar = İsviçre İmza Tüzüğü md. 18

Madde 18

SAS, Federal Konsey tarafından THG madde 14 uyarınca aktedilmiş milletlerarası anlaşmalar çerçevesinde akredite edilmiş yabancı sertifika hizmeti sağlayıcılarının listesini kamuya açar.

ALMAN İMZA KANUNU ve İMZA YÖNETMELİĞİ

1. 5070 Sayılı İmza Kanunu md. 6: Güvenli Elektronik İmza Oluşturma Araçları = Alman İmza Kanunu md. 17/1,2,3 = İmza Yönetmeliği md. 2, 15

Nitelikli Elektronik İmza Ürünleri (SigG md. 17)

- İmza anahtarlarının bloke edilmesi, ayrıca nitelikli elektronik imzanın hazırlanması için, imzadaki sahteciliklerı ve imzalanan datalardaki hileleri keşfetmeye yarayan ve imza anahtarını yetkili olmayan kullanımlara karşı koruyan güvenli imza hazırlama ünitelerinin kullanılması gerekir. İmza anahtarı bizzat güvenli bir imza hazırlama ünitesi kullanılarak hazırlanmışsa, bu durumda fıkra 3/b. 1 kıyasen uygulama alanı bulacaktır (SigG md. 17/f.1).
- İmzalanan dataların görülebilmesi için, nitelikli bir elektronik imzanın hazırlanmasında imzanın hangi datalara ilişkin olduğunu önceden açık bir şekilde göstermeye ve tespit ettirmeye yarayan imza uygulama bileşenleri gereklidir. İmzalanmış dataların kontrolü bakımından imza uygulama bileşeni,

1. imzanın hangi datalara ilişkin olduğunun,
2. imzalanmış dataların değiştirilip değiştirilmediğinin,
3. imzanın hangi imza anahtarı kullanıcısına tahsis edildiğinin,
4. imzanın dayandığı nitelikli sertifikanın ve ilgili nitelikli takma ad sertifikasının içeriğinin ne olduğunun, ve
5. sertifikaların tekrar kontrol edilmesinin md. 5/f.1,c.2'ye göre hangi sonuca götüreceğinin tespit ettirilmesi bakımından gereklidir.

İmza uygulama bileşenleri, gerekirse imzalanan veya imzalanmış olan dataların içeriğinin de yeteri ölçüde anlaşılabilmesini sağlamak zorundadır. İmza anahtarı sahibinin bu tür imza uygulama bileşenlerini kullanması veya nitelikli elektronik imzanın güvenliği için uygun olan diğer tedbirleri alması gerekir.

- Sertifika hizmeti için tasarlanan teknik bileşenlerin,

1. İmza anahtarlarının hazırlanmasında ve teslim edilmesinde, imza anahtarının tekliğinin ve gizliliğinin sağlanması ve güvenli imza hazırlama üniteleri haricinde yapılacak bir blokajı engellemek,
2. Madde 5/f.1, c.2'ye göre tekrar kontrol edilebilir veya iptal edilebilir durumda bulundurulan nitelikli sertifikayı yetkili olmayan değişikliklerden ve yine yetkili olmayan geri almalardan korumak, ayrıca
3. Nitelikli zaman kaşesinin hazırlanması sırasında ortaya çıkabilecek hileleri ve sahtecilikleri önlemek için tedbirler içermesi gerekir (SigG md. 17/f.3).

- Fıkra 1 ve 3/b.1'deki ve md. 24'e göre Yönetmelikte yer alan hususların yerine getirilip getirildiği bir makam tarafından md. 18'e göre tasdik edilmelidir. Fıkra 2 ve 3/b.2 ve 3'te yer alan taleplerin yerine getirilip getirilmediği konusunda ise nitelikli elektronik imza ürünlerinin üreticisi tarafından yapılacak bir beyan yeterlidir (SigG md. 17/f.4).

2. 5070 Sayılı İmza Kanunu md. 8: Sertifika Hizmet Sağlayıcı = Alman İmza Kanunu md. 4 = İmza Yönetmeliği md. 5

Genel Şartlar (SigG md. 4)

- Sertifika hizmeti veren bir kurumun işletilmesi için, bu Kanun çerçevesinde onaya gerek yoktur (SigG md. 4/f.1).
- Sertifika hizmeti sunan bir kurum ancak, işletme için gerekli güvenilirliğe ve uzman personele sahip olan, ayrıca md. 12'ye göre teminat yükümlülüğünü yerine getiren ve sertifika hizmeti verilebilmesi için bu Kanunun ve 24. maddesinin 1,3 ve 4. fıkralarına göre Yönetmeliğin aradığı diğer şartları yerine getiren kimseler tarafından işletilebilir. Gerekli güvenilirlik kavramı, sertifika hizmeti sunan kurum olarak işletme ile ilgili olan yasal kurallara uygun hareket edileceğini garanti etmeyi kapsamaktadır. Gerekli uzman personel kavramı, sertifika hizmetinin sunulmasında görev yapan kimselerin, bu faaliyet

için gerekli olan bilgiye, tecrübeye ve beceriye sahip olmalarını ifade etmektedir. Sertifika hizmetinin verilmesi için gerekli olan diğer şartlar ise, bu Kanuna ve 24. maddenin 1,3 ve 4. fıkralarına atfen Yönetmeliğe göre, güvenlik gereklerinin yerine getirilmesi için gerekli olan tedbirlerin yetkili makamlar tarafından bir güvenlik taslağı şeklinde gösterildiği ve işe yarar olduğu ve pratik olarak uygulanabildiği hallerde söz konusu olacaktır (SigG md. 4/f.2).

- Sertifika hizmeti sunan bir kurumu işletmek isteyen herhangi bir kimse, bunu yetkili makamlara en geç işletmeye başlamasıyla birlikte bildirmek zorundadır. Bildirimle birlikte, fıkra 2'nin aradığı şartların yerine getirildiği uygun bir şekilde gösterilmiş olmaktadır (SigG md. 4/f.3).
- Fıkra 2'nin aradığı şartların yerine getirildiği sertifika hizmetinin verildiği bütün süreç içerisinde garanti edilmelidir. Bunu imkansız kılan durumların varlığı gecikmeksizin yetkili makamlara bildirilmelidir (SigG md. 4/f.4).
- Sertifika hizmeti sunan bir kurum, fıkra 2, cümle 4'te ifade edilen kendi güvenlik taslağında belirtmiş olmak kaydıyla, bu Kanundan ve 24. maddeye göre Yönetmelikten doğan yükümlülüklerini bir üçüncü kişiye devredebilir (SigG md. 4/f. 5).

3. 5070 Sayılı İmza Kanunu md. 10: Sertifika Hizmet sağlayıcıların Yükümlülükleri = Alman İmza Kanunu md. 4, 5, 6, 8, 9, 10, 13, 14, 15 = İmza Yönetmeliği md. 3, 4, 5

Genel Şartlar (SigG md. 4)

- Sertifika hizmeti veren bir kurumun işletilmesi için, bu Kanun çerçevesinde onaya gerek yoktur (SigG md. 4/f.1).
- Sertifika hizmeti sunan bir kurum ancak, işletme için gerekli güvenilirliğe ve uzman personele sahip olan, ayrıca md. 12'ye göre teminat yükümlülüğünü yerine getiren ve sertifika hizmeti verilebilmesi için bu Kanunun ve 24. maddesinin 1,3 ve 4. fıkralarına göre Yönetmeliğin aradığı diğer şartları yerine getiren kimseler tarafından işletilebilir. Gerekli güvenilirlik kavramı, sertifika hizmeti sunan kurum olarak işletme ile ilgili olan yasal kurallara uygun hareket edileceğini garanti etmeyi kapsamaktadır. Gerekli uzman

personel kavramı, sertifika hizmetinin sunulmasında görev yapan kimselerin, bu faaliyet için gerekli olan bilgiye, tecrübeye ve beceriye sahip olmalarını ifade etmektedir. Sertifika hizmetinin verilmesi için gerekli olan diğer şartlar ise, bu Kanuna ve 24. maddenin 1,3 ve 4. fıkralarına atfen Yönetmeliğe göre, güvenlik gereklerinin yerine getirilmesi için gerekli olan tedbirlerin yetkili makamlar tarafından bir güvenlik taslağı şeklinde gösterildiği ve işe yarar olduğu ve pratik olarak uygulanabildiği hallerde söz konusu olacaktır (SigG md. 4/f.2).

- Sertifika hizmeti sunan bir kurumu işletmek isteyen herhangi bir kimse, bunu yetkili makamlara en geç işletmeye başlamasıyla birlikte bildirmek zorundadır. Bildirimle birlikte, fıkra 2'nin aradığı şartların yerine getirildiği uygun bir şekilde gösterilmiş olmaktadır (SigG md. 4/f.3).
- Fıkra 2'nin aradığı şartların yerine getirildiği sertifika hizmetinin verildiği bütün süreç içerisinde garanti edilmelidir. Bunu imkansız kılan durumların varlığı gecikmeksizin yetkili makamlara bildirilmelidir (SigG md. 4/f.4).
- Sertifika hizmeti sunan bir kurum, fıkra 2, cümle 4'te ifade edilen kendi güvenlik taslağında belirtmiş olmak kaydıyla, bu Kanundan ve 24. maddeye göre Yönetmelikten doğan yükümlülüklerini bir üçüncü kişiye devredebilir (SigG md. 4/f. 5).

Nitelikli Sertifikanın Verilmesi (SigG md. 5)

- Sertifika hizmeti sunan kuruluş, nitelikli sertifika verilmesi yönünde talepte bulunan kimselerin kimliklerini sıkı bir şekilde tespit etmek zorundadır. Ayrıca kimlik tespiti yapılmış bir kimseye imza kontrol anahtarının koordine edilmesini yine nitelikli bir sertifika vasıtasıyla teyit etmeli ve bunu her zaman, herkes için aleni olarak ulaşılabilen her türlü iletişim hatları üzerinden tekrar gözden geçirilebilir ve geri alınabilir bir şekilde hazır bulundurmalıdır. Nitelikli bir sertifika sadece imza anahtarı sahibinin onayı ile geri alınabilir (SigG md. 5/f.1).
- Nitelikli bir sertifika, talep sahibinin istemi üzerine üçüncü bir kişi için kendi temsil yetkisi ayrıca mesleki veya kendi kişiliği ile ilgili diğer açıklamaları içerebilir. Temsil yetkisi hakkındaki bilgiler açısından, üçüncü kişinin rızasının mevcudiyeti ispat edilmelidir; mesleki veya kişi ile ilgili diğer bilgilerin ise yetkili makamlar tarafından onaylanması gerekir. Üçüncü bir kişi için temsil yetkisi hakkındaki bilgiler sadece cümle

2'ye göre rızanın ispatı durumunda, mesleki veya talep sahibinin kişiliği ile ilgili diğer bilgiler ise sadece cümle 2'ye göre tasdik belgesinin ibrazı halinde nitelikli bir sertifikada yer alabilirler. Kişi ile ilgili diğer tüm bilgiler ise yine sadece ilgili kimsenin rızası ile nitelikli bir sertifikada yer alabilir (SigG md. 5/f.2).

- Sertifika hizmeti sunan kuruluş, talep sahibinin istemi üzerine nitelikli bir sertifikada talep sahibinin ismi yerine takma adını kullanabilir. Nitelikli bir sertifika üçüncü bir kişi için temsil yetkisi hakkındaki bilgileri veya mesleki veya kişi ile ilgili diğer bilgileri ihtiva ediyorsa, takma ad kullanımı için üçüncü kişinin veya mesleki veya diğer bilgiler için yetkili makamın rızası gereklidir (SigG md. 5/f.3).
- Sertifika hizmeti sunan kuruluş, nitelikli sertifikaya mahsus datalarda kasıtlı olarak yapılacak hilecilik ve sahtecilikleri önleyecek tedbirler almak zorundadır. Sertifika kuruluşu ayrıca imza anahtarının gizliliğini sağlayacak başka tedbirleri de almalıdır. Güvenli imza hazırlama ünitesinin dışında imza anahtarının kopyalanması yasaktır (SigG md. 5/f.4).
- Sertifika hizmeti sunan kuruluş, sertifikalandırma işleminin icrası için ve nitelikli elektronik imza için, asgari olarak bu Kanunun 4-14 ve 17 veya 23. ve 24. maddeye göre de Yönetmeliğin aradığı şartları taşıyan güvenilir personele ve ürünlere sahip olmak zorundadır (SigG md. 5/f.5).
- Sertifika hizmeti sunan kuruluş, talep sahibinin ilgili güvenli imza hazırlama ünitesine sahip olduğundan uygun bir şekilde kanaat sahibi olmak zorundadır (SigG md. 5/f.6).

Uyarı Yükümlülüğü (SigG md. 6)

- Sertifika hizmeti sunan kuruluş, talep sahibini md. 5/f.1'e göre nitelikli elektronik imzanın güvenliğini sağlamak ve yine bu imzanın güvenli bir şekilde kontrolünü gerçekleştirmek için gerekli olan tedbirler konusunda uyarmak zorundadır. Sertifika kuruluşu ayrıca mevcut imzanın güvenilirlik değeri zamanla azalacağı için, nitelikli elektronik imza ile imzalanmış olan dataların gerekirse yeniden imzalanması gerektiği konusunda talep sahibinin dikkatini çekmelidir (SigG md. 6/f.1).

- Sertifika hizmeti sunan kuruluş, kanun aksini öngörmediği sürece nitelikli elektronik imzanın hukuki ilişkilerde, aynen el yazısı ile atılan imza gibi hukuki sonuç doğuracağı konusunda talep sahibini uyarmak zorundadır (SigG md. 6/f.2).
- 1 ve 2. fıkralardaki bildirimlerin yapılması için, talep sahibine yazılı bir talimat verilmelidir. Talep sahibi bu talimatı aldığını ayrı bir imza ile teyit etmek zorundadır. Talep sahibi daha önceki bir zamanda 1 ve 2. fıkralar hakkında bilgilendirilmişse, yeni bir bildirime gerek olmayabilir (SigG md.6/f.3).

Nitelikli Sertifikanın Bloke Edilmesi (SigG md. 8)

- Sertifika hizmeti sunan kuruluş, sertifika md. 7'de istenilen hususlar yanlış bilgiler verilerek tanzim edilmişse, imza anahtarı sahibinin veya temsilcisinin talebi üzerine derhal nitelikli bir sertifikayı bloke etmek zorundadır. Sertifika hizmeti sunan kuruluş faaliyetine son verir ve bu faaliyet artık başka bir sertifika kuruluşu tarafından devam ettirilemez veya yetkili makam md. 19/f.4'e göre blokenin nasıl yapılacağını tayin eder. Blokaj, hangi andan itibaren geçerli ise, bu anı ihtiva etmek zorundadır. Geçmişe etkili bir blokaj geçerli değildir. Nitelikli bir sertifika yanlış bilgiler sonucu tanzim edilmişse, sertifika hizmeti sunan kuruluş ek olarak ayrıca bunu da açıklayabilir (SigG md. 8/f.1).
- Nitelikli bir sertifika md. 5/f.2'deki bilgileri içeriyorsa ve üçüncü kişiler veya mesleki veya kişi ile ilgili diğer bilgiler için aranan şartlar bu verilerin nitelikli sertifikaya kaydedilmesinden sonra değişmişse; mesleki veya kişi ile ilgili bu tür diğer veriler için yetkili makam dahi ilgili sertifikanın fıkra 1'e göre bloke edilmesini talep edebilir (SigG md. 8/f.2).

Nitelikli Zaman Kaşesi (SigG md. 9): Sertifika hizmeti sunan bir kurum nitelikli zaman kaşesi hazırlamışsa, md. 5/f.5 burada da benzer şekilde uygulama alanı bulacaktır.

Belgeleme (SigG md. 10)

- Sertifika hizmeti sunan kurum, bu Kanun ve md. 24/b.1,3, ve 4 hükümlerine göre Yönetmelik hükümlerine riayeti sağlayacak güvenlik tedbirlerini ve ayrıca hazırlanan nitelikli sertifikaları 2. cümle doğrultusunda, datalar ve gerçeklikleri her zaman için

kontrol edilebilecek şekilde belgelemek zorundadır. Belgelemenin, söz konusu belgelerde sonradan gizlice değişiklik yapılmasına olanak vermeyecek şekilde gecikmeksizin yapılması gerekir. Bu özellikle nitelikli sertifikanın hazırlanması ve bloke edilmesinde de geçerlidir (SigG md. 10/f.1).

- İmza anahtarı sahibine talep etmesi halinde kendisi ile ilgili datalar ve izlenen yöntem bakımından inceleme yetkisi verilir (SigG md. 10/f.2).

Faaliyetin Durdurulması (SigG md. 13)

- Sertifika hizmeti sunan kuruluş, faaliyetini durdurduğunu gecikmeksizin derhal yetkili makamlara bildirmek zorundadır. Sertifika hizmeti sunan kuruluş faaliyetine son verirken, geçerli nitelikli sertifikaların başka bir sertifika hizmeti sunan kuruluş tarafından kabul edilmesini veya bu sertifikaların bloke edilmesini sağlamak zorundadır. Sertifika hizmeti sunan kuruluş, imza anahtarı sahibine faaliyetini durdurması ve nitelikli sertifikaların başka bir sertifika hizmeti sunan kuruluş tarafından üstlenilmesi hakkında bilgi vermek zorundadır (SigG md. 13/f.1).
- Sertifika hizmeti sunan kuruluş, md. 10'a göre yaptığı belgelemeyi fıkra 1'e göre sertifikayı devralan, sertifika hizmeti sunan kuruluşa devretmek zorundadır. Herhangi bir sertifika hizmeti sunan kuruluş belgelemeyi üstlenmezse, yetkili makam bunu üstlenecektir. Yetkili makam haklı bir menfaatin varlığı durumunda, teknik olarak büyük bir külfet getirmediği sürece, belgeleme ile ilgili bilgi almaya izin verebilir (SigG md. 13/f.2).
- Sertifika hizmeti sunan kuruluş, aciz prosedürünün başlatılması yönündeki bir talebi derhal yetkili makama bildirmek zorundadır (SigG md. 13/f.3).

Bilginin Korunması (SigG md. 14)

- Sertifika hizmeti sunan kuruluş kişiye ilişkin olan dataları yalnızca doğrudan doğruya bizzat ilgiliye karşı ve nitelikli bir sertifikanın amacı için gerekli görüldüğü ölçüde kaldırabilir. Üçüncü kişilere karşı yapılacak bu tür bir bilgi ifşası ancak ilgilinin rızası ile mümkündür. Cümle 1'de anılan amacın dışındaki amaçlar için datalar ancak, kanun buna izin verdiği veya ilgili rıza gösterdiği sürece kullanılabilir (SigG md. 14/f.1).
- Takma ad kullanan bir imza anahtarı sahibi söz konusu olduğu durumda ise, sertifika hizmeti sunan kuruluş bu kişinin kimliği hakkındaki bilgileri; bir suçun veya kamu

düzenine aykırı bir davranışın kovuşturulması için, kamu düzenini veya kamu güvenliğini ihlal edecek tehlikelerin önlenmesi veya federal hükümetin ve eyaletlerdeki Anayasayı Koruyucu Kurumların, Federal istihbarat servisinin, askeri istihbarat servisinin veya mali kurumların yasal görevlerini ifa edebilmeleri için gerekli olduğu takdirde veya mahkemeler bu bilgilerin verilmesini derdest bir dava kapsamında, bu iş için geçerli olan hükümler çerçevesinde talep ettiği takdirde yetkili makama bildirmek zorundadır. Bilgilerin belgelenmesi gerekir. Talepte bulunan makam, bu sayede yasal yükümlülüklere riayet ihlal edilmemiş olacaksa veya imza anahtarı sahibinin bilgilendirilme konusunda üstün menfaati söz konusu ise; imza anahtarı sahibini, takma adının ifşa edildiği konusunda bilgilendirmelidir (SigG md. 14/f.2).

- Madde 2/b.8'de belirtilenlerden başka bir sertifika hizmeti sunan kuruluş elektronik imza için sertifika hazırlamışsa, 1 ve 2. fıkralar bu durumda da uygulama alanı bulacaktır (SigG md. 14/f.3).

Üçüncü Bölüm: İhtiyari Akreditasyon

Sertifika Hizmeti Sunan Kuruluşların İhtiyari Akreditasyonu (SigG md. 15)

- Sertifika hizmeti sunan kuruluş, yapacağı talep üzerine yetkili makam tarafından kendisini akredite ettirtebilir; yetkili makam akreditasyon için özel kurumlara başvurabilir. Sertifika hizmeti sunan kuruluş, bu Kanun ve md. 24'e göre Yönetmelik hükümlerinin yerine getirildiğini ispat ederse akreditasyon kabul edilir. Akreditasyonlu sertifika hizmeti sunan kuruluşa yetkili makam tarafından bir kalite belgesi verilir. Bu belge ile birlikte, sertifika hizmeti sunan kuruluşun nitelikli sertifikasına dayanan nitelikli elektronik imza için, kapsamlı olarak kontrol edilen teknik ve idari güvenliğin yeterli ölçüde sağlandığı ifade edilmiş olmaktadır. Sertifika hizmeti sunan kuruluş bundan böyle Akreditasyonlu sertifika hizmeti sunan kuruluş olarak nitelendirilebilir ve gerek hukuki gerek iş ilişkilerinde kanıtlanmış olan güvenliğine istinat edebilir (SigG md. 15/f.1).
- Fıkra 1'e göre aranan şartların yerine getirilebilmesi için, madde 4/f.2,c.4'de ifade edilen güvenlik taslağının, madde 18'e göre bir makam tarafından uygunluğu ve somut olarak uygulanabilirliği açısından kapsamlı olarak kontrol edilmesi ve onaylanması gerekir. Bu kontrol ve onaylama işleminin güvenlik açısından önemli değişikliklerden sonra ve ayrıca düzenli zaman aralıkları içinde tekrarlanması gerekir (SigG md. 15/f.2).

- Sertifika hizmeti sunan kuruluşun faaliyete başlama ve faaliyetinin devamı sırasında, bu Kanunun ve md. 24'e göre Yönetmeliğin aradığı şartların yerine getirilmesini garanti etmek için gerekli görüldüğü takdirde, akreditasyonun yan hükümleri ile birlikte onaylanması gerekir (SigG md. 15/f.3).
- Bu Kanunun ve md. 24'e göre Yönetmeliğin aradığı şartlar yerine getirilmemişse, akreditasyon reddedilir; md. 19 burada kıyasen uygulanır (SigG md. 15/f.4).
- Bu Kanundan ve 24. Maddeye göre Yönetmelikten doğan yükümlülüklerin ifa edilmemesi halinde veya fıkra 4'e göre bir red sebebinin mevcudiyeti durumunda yetkili makam akreditasyonu kaldırabilir veya bu sebeplerin daha akreditasyon anında mevcut olması halinde, eğer md. 19/f.2'ye göre alınan tedbirler başarı şansı vaad etmiyorsa, akreditasyonu iptal edebilir (SigG md. 15/f.5).
- Bir akreditasyonun geri alınması veya iptali akreditasyonlu bir sertifika hizmeti sunan kuruluşun faaliyetinin durdurulması durumunda yetkili makam, faaliyetin başka bir akreditasyonlu sertifika hizmeti sunan kuruluş tarafından üstlenilmesini veya sözleşmelerin imza anahtarı sahibi ile birlikte tasfiye edilmesini güvence altına alması gerekir. Eğer faaliyet devam ettirilmeyecekse; aynı şey, aciz prosedürünün başlatılması talebi durumunda da geçerlidir. Herhangi bir akreditasyonlu sertifika hizmeti sunan kuruluş md. 13/f.2'ye göre belgelemeyi üstlenmezse, bu işi yetkili makam üstlenecektir. Madde 10/f.1,c.1 burada da benzer şekilde uygulama alanı bulacaktır.
- Nitelikli elektronik imza ürünleri bakımından, md. 17/f.1-3 ve md. 24'e göre Yönetmeliğin aradığı koşulların yerine getirilip getirilmediği, bilim ve tekniğin durumuna göre yeteri ölçüde kontrol edilmeli ve bir makam tarafından md. 18'e göre tasdik edilmelidir; fıkra 1/c.3 burada kıyasen uygulama alanı bulacaktır. Akreditasyonlu sertifika hizmeti sunan kuruluş,

1. kendi sertifika faaliyeti için, sadece cümle 1'e göre kontrol edilmiş ve onaylanmış ürünleri nitelikli elektronik imza için kullanmalıdır,
2. nitelikli sertifikayı sadece, cümle 1'e göre ispat edilebilir bir şekilde kontrol edilmiş ve onaylanmış güvenli imza hazırlama ünitelerine sahip olan kişiler için hazırlamak durumundadır, ve
3. imza anahtarı sahibini md. 6/f.1 çerçevesinde, cümle 1'e göre kontrol edilmiş ve onaylanmış imza uygulama bileşenleri hakkında bilgilendirmelidir.

4. 5070 Sayılı İmza Kanunu md. 11: Sertifikaların İptal Edilmesi = Alman İmza Kanunu md. 8 = İmza Yönetmeliği md. 7

Nitelikli Sertifikanın Bloke Edilmesi (SigG md. 8)

- Sertifika hizmeti sunan kuruluş, sertifika md. 7'de istenilen hususlar yanlış bilgiler verilerek tanzim edilmişse, imza anahtarı sahibinin veya temsilcisinin talebi üzerine derhal nitelikli bir sertifikayı bloke etmek zorundadır. Sertifika hizmeti sunan kuruluş faaliyetine son verir ve bu faaliyet artık başka bir sertifika kuruluşu tarafından devam ettirilemez veya yetkili makam md. 19/f.4'e göre blokenin nasıl yapılacağını tayin eder. Blokaj, hangi andan itibaren geçerli ise, bu anı ihtiva etmek zorundadır. Geçmişe etkili bir blokaj geçerli değildir. Nitelikli bir sertifika yanlış bilgiler sonucu tanzim edilmişse, sertifika hizmeti sunan kuruluş ek olarak ayrıca bunu da açıklayabilir (SigG md. 8/f.1).
- Nitelikli bir sertifika md. 5/f.2'deki bilgileri içeriyorsa ve üçüncü kişiler veya mesleki veya kişi ile ilgili diğer bilgiler için aranan şartlar bu verilerin nitelikli sertifikaya kaydedilmesinden sonra değişmişse; mesleki veya kişi ile ilgili bu tür diğer veriler için yetkili makam dahi ilgili sertifikanın fıkra 1'e göre bloke edilmesini talep edebilir (SigG md. 8/f.2).

5. 5070 Sayılı İmza Kanunu md. 14: Yabancı Sertifikalar = Alman İmza Kanunu md. 23 = İmza Yönetmeliği md. 18

Başka Bir Devlete Ait Elektronik İmzalar ve Elektronik İmza Ürünleri (SigG md. 23)

- Avrupa Topluluğuna üye diğer bir ülke veya Avrupa Ekonomik Pazarı Hakkındaki Anlaşmaya üye diğer bir devlet tarafından, hakkında yabancı nitelikli bir sertifika düzenlenmiş olan elektronik imzalar, Avrupa Parlamentosunun 1999/93/EG tarihli Yönergesinin md. 5/f.1'inin ve Avrupa Topluluğu Konseyinin Elektronik İmzalar İçin Topluluğa İlişkin Çerçeve Şartlar hakkındaki 13 Aralık 1999 tarihli Yönergesinin (ABI. EG 2000 Nr. L 13 S. 2) mevcut metnine uydukları takdirde, nitelikli elektronik imzalarla

eş değerli tutulacaklardır. Bunun dışında bir üçüncü ülkeye ait olan elektronik imzalar, ancak o ülkede yer alan bir sertifika hizmeti sunan kuruluş tarafından açıkça nitelikli sertifika olarak tanzim edilmişse ve 1999/93/EG tarihli Yönergenin md. 5/f.1 hükmü anlamında bir elektronik imzaya mahsussa ve

1. sertifika hizmeti sunan kuruluş Yönergenin aradığı koşulları yerine getirmişse ve Avrupa Topluluğuna üye bir devlette veya Avrupa Ekonomik Pazarı Hakkındaki Anlaşmaya üye diğer bir devlette akredite olmuşsa, veya
2. Topluluk içinde yerleşik ve Yönergenin aradığı şartları yerine getirmiş olan bir sertifika hizmeti sunan kuruluş, sertifika için garanti vermişse, veya
3. Avrupa Topluluğu ve bunun dışında kalan üçüncü gurup devletler veya uluslararası organizasyonlar arasında akdedilen iki veya çok taraflı anlaşmalarla, sertifika veya sertifika hizmeti sunan kuruluşun tanınmış olması halinde nitelikli elektronik imza ile eş değerli olarak kabul edilir (SigG md. 23/f.1).

- Birinci fıkraya göre elektronik imza, eğer eş değerli bir güvenliğe sahip olduğunu ispat edilebilir bir şekilde ortaya koyabiliyorsa, md. 15/f.1 anlamında sunucu akreditasyonlu nitelikli elektronik imza ile eş değerlidir (SigG md. 23/f.2).
- Elektronik imza ürünleri bakımından ise, Avrupa Topluluğuna üye diğer bir devlette veya Avrupa Ekonomik Pazarı Hakkındaki Anlaşmaya üye diğer bir devlette, 1999/93/EG tarihli Yönergenin gereklerini yerine getirdiği tespit edilen ürünler kabul edilecektir. Madde 15/f.7'ye göre kontrol edilen nitelikli elektronik imza ürünleri ise, eğer eş değerli bir güvenliğe sahip olduğunu ispat edilebilir bir şekilde ortaya koyarsa, 1. Cümlede anılan devlette veya üçüncü bir devletteki elektronik imza ürünleri ile eş değerli kabul edilecektir (SigG md. 23/f.3).

ALMAN İMZA YÖNETMELİĞİNİN İLGİLİ HÜKÜMLERİ

Bildirimin Şekli, İçeriği ve Bildirimde Yapılacak Değişiklikler (md. 1)

Elektronik imza kanunu md. 8/f.1 ve 2'ye göre yapılacak bildirim yazılı olarak veya elektronik imza kanunu anlamında nitelikli elektronik imza ile imzalanmış olarak kuruma ibraz edilecektir.

Bildirimin aşağıdaki bilgi ve belgeleri kapsaması zorunludur:

1. Sertifika Hizmet sağlayıcının adı ve adresi
2. yasal temsilcilerin isimleri
3. güncel bir ticaret sicil kaydı belgesi veya bu nitelikte diğer bir belge
4. gerekli teknik, idari ve hukuki branş bilgisine sahip olunduğunun ispatı
5. üçüncü kişilere yetki devri olasılığı da dahil olmak üzere ayrıntılı bir güvenlik taslağı, güvenlik taslağının nasıl uygulanacağı

Bend 1 ve 2'deki şartlar veya b. 5'deki güvenlik açısından aranan şartlarda değişiklik olduğunda, kuruma yazılı olarak veya imza kanunu anlamında nitelikli bir elektronik imza ile imzalı doküman şeklinde bilgi vermek gereklidir.

Güvenlik Taslağının İçeriği (md. 2)

Güvenlik Taslağı içerisinde aşağıdaki şu bilgilerin yer alması gereklidir:

1. Gerekli tüm teknik, yapısal (inşai) ve düzenleyici güvenlik tedbirlerinin ve bunların uygunluklarının açıklanması
2. nitelikli elektronik imza için kullanılan ürünlerin imalatçı beyanları ile birlikte beyan edilmesi
3. sertifika hizmetinin kuruluşu ve işleyişi
4. özellikle acil durumlarda geçerli olmak üzere hizmetin güvenliğini ve devamlılığını sağlayacak tedbir ve önlemler

5. çalıştırılan personelin güveinilirliğinin değerlendirilmesi ve bunun devamının sağlanması usulü (personel seçiminde ve denetiminde alınan güvenlik tedbirleri anlaşılıyor)
6. tekniğin ilerlemesine bağlı olarak ortaya çıkabilecek güvenlik risklerinin öngörülmesi ve değerlendirilmesi

Kimlik Tespiti (md. 3)

Sertifika hizmet sağlayıcı talep sahibinin kimliğini, nüfus cüzdanı veya pasaport veya eşdeğerli güvenilirliğe sahip diğer bir belgeye istinaden tespit etmelidir. Nitelikli bir sertifika talebi imza sahibi tarafından, imza kanununun aradığı anlamda nitelikli elektronik imza ile imzalanmış bir doküman aracılığıyla yapılırsa, sertifika hizmet sağlayıcı bir daha, yeniden kimlik tespiti yapmaktan kaçınabilir. Kimlik tespiti nitelikli sertifikanın tesliminden önce ve sertifika fihristine kayıttan önce yapılmalıdır.

Nitelikli bir sertifika içinde üçüncü kişiye bir temsil yetkisi verilecekse, bunun için gerekli olan rızanın veya onayın imza kanunu anlamında nitelikli bir elektronik imza ile imzalanan elektronik doküman şeklinde veya yazılı olarak (ıslak imzalı) verilmesi gerekir. Üçüncü kişi veya kişi ile ilgili mesleki veya diğer bilgiler yetkili makama imza kanununa göre nitelikli bir elektronik imza ile imzalanmış elektronik doküman şeklinde veyaz yazılı olarak, nitelikli elektronik imzanın içeriği hakkında bilgi verilerek ve blokaj imkanına da dikkat çekilerek yapılacaktır.

Sertifika Fihristlerinin Tutulması (md. 4)

Sertifika hizmet sağlayıcı tanzim ettiği sertifikaların, tanzim tarihinden itibaren, her bir sertifikada belirtilen geçerlilik süresi boyunca ve aynı zamanda sertifikanın geçerliliğinin sona erdiği yılın bitiminden itibaren 5 sene boyunca bu bilgileri ihtiva eden bir fihrist tutmalıdır.

Akreditasyonlu Sertifika Hizmet Sağlayıcılarda bu süre 30 yıldır.

Bilgilendirmenin İçeriği (md. 6)

İmza kanunu md..... göre talep sahibinin bilgilendirilmesi herkes tarafından anlaşılabilecek bir dilde ve en az aşağıdaki kapsamda yapılmalıdır:

1. Güvenli imza oluşturma ünitelerinin saklanması ve kullanılması ve kayıp durumlarında veya kötüye kullanma şüphesinin mevcudiyeti halinde alınacak uygun önlemler
2. Güvenli imza oluşturma ünitesi karşısında imza anahtarı sahibinin teşhisine yarayan kimlik numarası veya diğer bilgilerin saklanması (gizliliği)
3. Nitelikli elektronik imzanın oluşturulması ve kontrolünde gerekli olan güvenlik tedbirleri
4. nitelikli sertifikanın içeriği ile ilgili md....'a göre nitelikli sertifikada yapılabilecek sınırlandırma olasılıkları
5. imza, sürenin dolması nedeniyle güvenlik değerini kaybettiğinde, verilerin nitelikli elektronik imza ile yeniden imzalanmasının gerekliliği
6. talep sahibinin sahip olduğu itiraz ve uyuşmazlıkların alternatif çözüm yolları olasılıkları ve ayrıca bu yöntemlerin kullanılmasına ilişkin ayrıntılar
7. md.....'a göre yapılacak blokaj.

Bilgiler talep halinde üçüncü kişilerin erişimine de hazır bulundurulur.

Nitelikli Sertifikaların Bloke Edilmesi (md. 7)

Sertifika hizmet sağlayıcı, imza kanunu md....'e göre kişilerin derhal (gecikmeksizin) nitelikli sertifikaların blokajını sağlayabileceklerini bir çağrı numarasını, blokaj için yetkili kimselere verecektir.

Sertifika hizmet sağlayıcı blokajdan önce, blokaja yetkili olan kişilerin kimliği hakkında kanaat sahibi olmalıdır. Nitelikli sertifikanın blokajı, sertifika listesinde blokajın yapıldığı tarih ve saat gösterilerek kaydedilir.

Belgelemenin (Dokümantasyon) Kapsamı (md. 8)

1. İmza kanunu md.....'göre yapılacak belgeleme, güvenlik taslağını, tüm değişiklikleri, işletmede çalışan personelin branş bilgisine ilişkin belgeleri ve talep sahibi ile akdi olarak yapılan anlaşmaları kapsamalıdır.
2. İlgili talep sahibi için asgari olarak aşağıdaki bilgi ve belgelerin belgelenmesi gerekir:

    a) ibraz edilen nüfus cüzdanı ve diğer kimlik belgelerinin bir örneği
    b) kullanılan takma ad
    c) imza kanunu md.....'e göre talep sahibinin bilgilendirildiğinin iapatına yarayan belgeler
    d) imza kanunu md....'e göre yetkili kişilerin rızalarının ispatına ilişkin belgeler
    e) imza kanunu md.....'e göre yetkili makam tarafından verilen onaylar
    f) tanzim tarihi ve teslim tarihi ve ayrıca sertifika fihristine kayıt tarihi ile birlikte düzenlenen nitelikli sertifikalar
    g) nitelikli sertifikaların bloke edilmesi
    h) imza kanunu md....'e göre imza anahtarı ve kimlik bilgileri için devir onayları veya imza anahtarı sahibi başka bir devir (teslim) şekli talep etmişse, imza anahtarı sahibinin açıklamaları ve gerekirse diğer bir iapat şekli.

Belgelemenin md. ...'de belirtilen süre içinde ve akreditasyonlu Sertifika hizmet sağlayıcılarında ise en azından md.....'de belirtilen süre zarfında saklanması gerekir. Sertifikalandırmanın ispatının önemli olduğu bir dava durumunda ise, dokümantasyonun en azından dava kesin hükme bağlanana kadar muhafaza edilmesi gerekir. Müracaatların dokümantasyonunun ise 12 ay saklanması gerekir.

Faaliyetin Durdurulması (md. 10)

Sertifika hizmet sağlayıcı md....'e göre faaliyetine son verdiği tarihten en geç iki ay önce yetkili makama bildirimde bulunmalıdır.

Sertifika hizmet sağlayıcı imza kanunu md.....e göre imza anahtarı sahibine işi bırakmadan en az iki ay önce bildirimde bulunmak zorundadır. Sertifika hizmet sağlayıcı ayrıca imza sahibine, diğer bir sertifika hizmet sağlayıcının sertifikaları üstlenip üstlenmediğini de bildirmek ve üstlenmişse bunu belirtmek (tayin etmek) zorundadır.

Nitelikli Sertifikaların İçeriği ve Geçerlilik Süresi (md. 14)

İmza kanunu md....'deki bilgilerin nitelikli bir sertifikada açık bir şekilde yer alması gerekir.

Nitelikli bir Attribut sertifikanın, esasını teşkil eden nitelikli sertifikaya yapacağı açık atıf dışında en azından aşağıdaki şu bilgileri ihtiva etmesi ve Sertifika Hizmet sağlayıcının nitelikli elektronik imzasını taşıması gerekir:

1. sertifika hizmet sağlayıcının imza kontrol anahtarının kullanılacağı algoritmaların gösterilmesi
2. attribut sertifikanın numarası
3. sertifika hizmet sağlayıcının ve yerleşik olduğu devletin adı
4. nitelikli bir sertifikanın söz konusu olduğuna dair bilgiler ve
5. imza kanunu md..... göre bir veya birden çok attribut

Nitelikli bir sertifikanın geçerlilik süresi maksimum 5 yılı kapsamalıdır ve kullanılan algoritmaların uygunluk süresi ve ilgili parametrelerin aşılmaması gerekir. Nitelikli bir attribut sertifikanın geçerliliği en geç dayandığı nitelikli sertifika ile birlikte sona erer.

Nitelikli Elektronik İmza Ürünleri İçin Aranan Gereklilikler (md. 15)

İmza kanunu md.....'e göre; güvenli imza oluşturma ünitelerinin, imza anahtarının ancak imza sahibinin mülkiyet veya malumat (bilgi) veya bir veya birden çok biyometrik özellik yardımıyla teşhis edildikten sonra kullanılabilmesini güvence altına alması gerekir. İmza anahtarı ifşa edilemez. Biyometrik özelliklerin kullanımında imza anahtarının yetkisiz kullanımının yeteri ölçüde bertaraf edilmiş olması gerekir ve bilgiye dayalı bir yöntemin eşdeğerli bir güvenlik sağladığı hususunun yeteri ölçüde temin edilmiş olması gerekir. İmza anahtarlarının oluşturulması ve devri için gerekli olan teknik bileşenlerin, bir imza kontrol anahtarı veya bir imzanın imza anahtarı olarak ERRECHNEN yapılamayacağını garanti etmesi ve imza anahtarının çoğaltılmasını engellemesi gerekir.

İmza uygulama bileşenlerinin

1. nitelikli bir elektronik imzanın oluşturulmasında
   a)kimlik bilgilerinin ifşa edilmemesini ve bu bilgilerin sadece ilgili güvenli imza oluşturma ünitesine kaydedilmesini
   b) imzanın sadece yetkili olan kişi tarafından kullanılmasını
   c)imzanın oluşturulmasının önceden açıkça bildirilmesini güvence altına alması gerekir.

2. Nitelikli elektronik imzanın kontrolü sırasında
   a)imzanın doğruluğunun güvenilir bir şekilde kontrol edilmesini ve
   b) kontrol edilen nitelikli sertifikaların ilgili sertifika fihristinde iddia edilen zamanda mevcut olup olmadığının ve bloke edilip edilmediğinin açıkça fark edilebilmesini sağlamalıdır.

3. md.....göre teknik bileşenlerin bu sertifikaların doğruluğu hakkındaki bilgilerin kontrol edilebilmesini sağlaması gerekir. Cümle 1'e göre kontrol edilen nitelikli sertifikanın iddia edilen zamanda nitelikli sertifika fihristinde mevcut olup olmadığı ve bloke edilip edilmediğini ihtiva etmesi gerekir.
4. teknik bileşenlerde güvenlik tekniği açısından söz konusu olabilecek değişikliklerin kullanıcı tarafından fark edilebilir olması sağlanmalıdır
5. md.....'e göre bir üretici beyanının

a)imalatçıyı ve ürünü doğru olarak nitelemesi

b) Bu yönetmeliğin ve kanunun aradığı hangi gerekliliklerin ayrıntılı olarak yerine getirildiği hakkında detaylı bilgileri ihtiva etmesi gerekir.

Ürünlerin güvenilirliklerinin kontrol edilmesi ve onaylanmasında EK 1 Bölüm 2'deki hususların dikkate alınması gerekir.

Yabancı Elektronik İmzalar ve Elektronik İmza ürünlerinin Güvenilirliklerinin Eşdeğerliliğinin Tespit Edilmesi Yöntemi (md. 18)

İmza Kanunu md.....'e göre bir sertifika hizmet sağlayıcı, AB dışında yerleşik bir sertifika hizmet sağlayıcının nitelikli sertifikaları için, 1999/93/EG Yönergesinin md. 5/f.1'i anlamında hukuki sonuç doğuracak şekilde garanti verirse, bu durumda yetkili makama en geç, bu sertifikaların imza kanununun geçerlilik alanında hukuki etkiye sahip olmaları gereken zamanda yazılı olarak veya imza kanunu anlamında nitelikli elektronik imza ile imzalanmış elektronik bir doküman şeklinde bildirimde bulunmak gereklidir. Garanti eden sertifika hizmet sağlayıcı ayrıca yabancı sertifika hizmet sağlayıcının nitelikli sertifikaları ve buna istinad eden nitelikli elektronik imzaların, imza kanununun ve bu yönetmeliğin aradığı şartları taşımasını ve yabancı sertifika hizmet sağlayıcıya md. 1 f.2'ye uygun olarak belgelerin ibraz edilmesini sağlamak durumundadır. Md. 2 yabancı sertifika hizmet sağlayıcıya yapılacak bildirimler bakımından da benzer şekilde uygulama alanı bulacaktır.

Yabancı elektronik imzaların eşdeğerli güvenlik koşullarını sağladığı yetkili makamın şu aşağıdaki koşulların mevcut olduğunu tespit etmesi halinde kabul edilecektir:

1. sertifika hizmet sağlayıcısına ve nitelikli elektronik imza ürünlerine yönelik güvenlik kriterleri
2. sertifika hizmet sağlayıcının ve nitelikli elektronik imza ürünlerinin denetim (kontrol) yöntemleri ve ayrıca kontrol ve tasdik makamlarına yönelik gereklilikler
3. akreditasyon ve denetim sistemi eşdeğerli güvenliği sağlıyorsa.

Yetkili makam imza kanunu md.....göre tutacağı fihristte, imza kanunu md.....göre eşdeğerli olarak kabul edilen en üst yabancı sertifika hizmet sağlayıcının imza anahtarı için kullanılan nitelikli sertifikalara da yer vermek zorundadır.

EK

I. SigV m. 11/f.3 ve SigG m. 15/f.7:

1. Kontrol Kriterleri

1.1. Kontrolde Uyulması Gereken Kriterler

SigG m.15/f.7 ve m. 17/f.4 uyarınca nitelikli elekronik imzalarda kullanılan araçların denetiminde "Enformasyon teknolojisi güvenliğinin kontrol ve değerlendirilmesinde bileşik kriterler" (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, - ISO/IEC 15408) ya da "Enformasyon teknolojisi sistemlerinin güvenliğinin değerlendirilmesinde kriterler" (ITSEC-GMBl 8.08.1992, S.545)'in güncel versiyonu dikkate alınmalıdır.

Kontrol, asgari olarak,

a) SigG m. 2/b.12 (a) uyarınca teknik bileşenlerde EAL 4 veya E 3 kontrol derinliğini taşımalıdır.

b) SigG m. 2/b.10 uyarınca güvenli imza oluşturma ünitelerinde EAL 4 veya E 3 kontrol derinliğini taşımalıdır.

c) i) SigG m. 2/b.12 (b) ve (c) uyarınca özellikle korunaklı alanların ("Trustcenter") dışında kullanılan sertifika hizmetlerinin teknik bileşenleri EAL 4 veya E 3 kontrol seviyesine uygun olmalıdır.

ii) SigG m. 2/b.12 (b) ve (c) uyarınca özellikle korunaklı alanların ("Trustcenter") içinde kullanılan sertifika hizmetlerinin teknik bileşenleri EAL 3 veya E 2 kontrol seviyesine uygun olmalıdır.

d) SigG m. 2/b.11 uyarınca imza oluşturma bileşenleri EAL 3 veya E 2 kontrol seviyesine uygun olmalıdır.

1.2. Zayıf Alanların Değerlendirilmesinde Aranan Kriterler

Ekte bölüm I No. 1.1. bent a)'dan c) i)'ye kadar ve bent d)'de belirtilen durumlarda EAL 4 ve EAL 3 kontrol seviyelerinin öngördüğü tedbirlerin yanı sıra yüksek saldırı potansiyeline karşı kontrol edilmeli ve tümel bir kötüye kullanım analizi yapılmalıdır.

Bölüm I No. 1.1. bent a)'dan d)'ye kadar yer alan hükümlerin uygulama alanına giren tüm ürünlerde E3 ve E2 güvenlik mekanizmalarının gücü "yüksek" olarak değerlendirilmelidir. Tanımlamada bilgi verileri dışında biyometrik yöntemlerin de kullanılması halinde ise, güvenlik mekanizmalarının güvenlik gücünün "orta"ile değerlendirilmesi yeterli olacaktır.

1.3. Algoritmalarda Aranan Kriterler

Algoritmalar ve ilgili parametreler ek Bölüm I No: 1.2 uyarınca "uygun" olarak kabul edilmelidir.

2. Algoritmalar – Uygunluğun Yayınlanması

İmza anahtarlarının oluşturulmasında, imzalancak verilerin "hash" edilmesinde veya nitelikli elektronik imzaların oluşturulmasında ve denetlenmesinde uygun kabul edilen algoritma ve ilgili parametreleri gösteren tablolar ile geçerliliklerinin sona ereceği tarih yetkili makam tarafından Resmi Gazete'e yayınlatılmalıdır. Yayınlanacak tarih her halde değerlendirme ve yayınlama tarihinden itibaren 6 yıl sonra olmalıdır. Uygunluk gerektiğinde her yıl yeniden değerlendirilmelidir. Gösterilen tarih aralığında nitelikli

elektronik imzaların tespit edilemeyecek surette sahte olarak çoğaltılması olasılığının veya imzalanan verilerin sahte surette değiştirilmesi halinin tekniğin ulaştığı düzey ile imkansızlığının tespit edilmesi uygunluğun tanımlanmasında dikkate alınır. Uygunluk uluslararası standartlar dikkate alınarak Telekomünikasyon Kurumu'nun açıklayacağı standartlar uyarınca tespit edilecektir. Bu değerlendirmelerde bilim ve ticaret dünyasından uzmanların görüşleri de dikkate alınmalıdır.

3. İmza Ürünleri için Güvenlik Tasdiki

Nitelikli elektronik imzaların oluşturulmasında kullanılan ürünler hakkında düzenlenecek uygunluk belgesinin aşağıdaki şartları taşıması gerekecektir:

a) Hangi kriterler için SigG m. 17 ve Yönetmelik m. 15 uyarınca hazırlanan tasdik belgesinin geçerli olacağı ve hangi kullanım şartlarında,
b) Hangi algoritmalar ve ilgili parametrelerin kullanılacağı ve bunların hangi zaman dilimi içinde uygun kabul edileceği,
c) ürünlerin hangi seviyeye göre denetlendiği ve hangi mekanizma derecesine ulaşıldığı

bilgilerine yer verilmelidir.

Kontrol raporunu, tasdik makamının değerlendirmesi ve tasdiki ile beraber yetkili makama sunması gereklidir. Talep halinde ayrıca diğer kontrol belgeleri de sunulmalıdır. Yetkili makam kontrolde veya tasdik edilen ürünlerde eksiklik görürse, yapılan kontrolün ekte yer alan kriterlere göre yapılıp yapılmadığı ve SigG ile SigV uyarınca yeterli olup olmadığı konusunda üçüncü bir kişinin görüşüne de müracaat edebilecektir. İlgili üreticiler, dağıtıcılar ve kontrol yerleri gerekli desteği sağlamakla yükümlü olacaktır. Bu destek sağlanmaz ise veya tasdik edilen ürünlerin yeterli şekilde kontrol edilmediği veya aranılan kriterlere uygun olmadığı anlaşılırsa, yetkili makam verilen tasdiklerin geçersizliğine karar verebilecektir.

4. Ürün Güvenlik Tasdiklerinin Yayınlanması

SigG m. 18 uyarınca tanınan bir birimden Ek Bölüm I No. 3 gereğince nitelikli elektronik imzaların oluştururlmasında kullanılan ürünlerin tasdiki, yetkili makam (Telekomünikasyon Kurumu) tarafından Resmi gazete'de yayınlanmalıdır. Yayında

tasdikin geçerli olacağı süre de belirtilmelidir. Eğer verilen bir tasdik geçersiz olarak kabul edilirse, bu halde yetkili makam bunu tedbirin geçerli olacağı zamanı da belirterek Resmi gazete'de yayınlamalıdır.

EK – 2 : KAYNAKÇA

Thomas J. Smedinghoff, CERTIFICATION AUTHORITY *LIABILITY ANALYSIS,* American Bankers Association Publications, Illinois, 2001.

Interdisciplinary Centre for Law & Technology; K.U. Leuven, Landwell Law Firms, The Implementation of The European Directive on Electronic Signature, Belgium, Status Report September 2002.

4. Jos Dumortier, Stefan Kelm, Hans Nilsson, Georgia Skouma, Patrick Van Eecke, The Legal and Market Aspects of Electronic Signatures, Study For The European Commission – DG Information Society Service Contract Nr. C 28.400, Brussels, 2003.

Infocomm Development Authority of Singapore, Security Guidelines for Certification Authorities – Version 2.0, Singapore, September 2003.

Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, American Bar Association, PKI Assessment Guidelines, American Bar Association Publishing, Chicago, 2001.

Erdal Yıldız, A Proposal For Turkish Government Public Key Infrastructure Trust Model, Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2001.

Kathy Lyons-Burke, Computer Security - Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, NIST Special Publication 800-25, U.S. Goverment Printing Office, Washington, 2000.

Shimshon Berkovits, Santosh Chockhani, Judith A. Furlong, Jisoo A. Geiter, Jonathan J. Guild, Public Key Infrastructure Study, National Institute of Standards and Technology, Virginia, 1994.

ETSI, Electronic Signature Standardization For Business Transactions, Valbonna – France, 2000.

Interdisciplinary Center For Law And Information Technology, The Legal Aspects of Digital Signatures, European Commission, Brussels, October 1998.

Steffen Hindelang, No Remedy for Disappointed Trust – The Liability Regime for Certification Authorities Towards Third Parties Outwit the EC Directive in England and Germany Compared, Journal of Information, Law and Technology – Issue I, 22 Marc 2002 (JILC 02/1), Warwick.

ETSI, Policy Requirements For Certification Authorities Issuing Qualified Certificate, Valbonna – France, 2000.

ETSI, Qualified Certificate Profile, Valbonna – France, 2000.

ETSI, Time Stamping Profile, Valbonna – France, 2000.

ETSI, Electronic Signatures and Infrastructures (ESI); Policy Requirements For Certification Service Provider Issuing Attribute Certificate Usable With Qualified Certificates, Cedex – France, 2003.

ETSI, International Harmonization of Policy Requirements For CAs issuing certificates, Cedex – France, 2003.

ETSI, Electronic Signatures and Infrastructures (ESI); Signature Policy For Extended Business Model, Cedex – France, 2003.

ETSI, Time Stamping Profile, Cedex – France, 2002.

ETSI, Electronic Signatures and Infrastructures (ESI); Policy Requirements For Time Stamping Authorities, Cedex – France, 2003.

ETSI, Electronic Signatures and Infrastructures (ESI); Provision of Harmonized Trust Service Provider Status Information, Cedex – France, 2003.

ETSI, Provision of Harmonized Trust Service Provider Status Information, Cedex-France, 2002.

ETSI, Signature Policies Report, Cedex – France, 2002.

ETSI, Policy Requirements For Certification Authorities Issuing Qualified Certificates, Cedex – France, 2002.

ETSI, Qualified Certificate Profile, Cedex – France, 2001.

ETSI, Policy Requirements For Certification Authorities Issuing Public Key Certificates, Cedex – France, 2002.

ETSI, Time Stamping Profile, Cedex – France, 2000.

Aalberts, B.P.; Van Der Hof, S., Digital Signature Blindness, Analysis of Legislative Approaches To Electronic Authentication, Electronic Communication Law Review, 7 (1); 2000, Kluwer Law International, S. 1-55.

Kuner, Christopher; Meindbredt, Anja, Written Signature Requirements and Electronic Authentication; A Comparative Respective, Electronic Communication Law Review 6 (2/3); 1999, Kluwer Academic Publishers, S. 143 – 154.

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

Braley, Sarah Wood, Why Electronic Signature Can Increase Electronic Transaction and The

Need For Laws Governing Electronic Signatures, NAFTA; Law and Business Review of Americas 7 (3); Summer 2001, Kluwer Academic Publishers, S. 417 – 444.

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

Mitrakas, Andreas, Legal Aspects of Time Stamping, Electronic Communication Law Review 8 (1); 2001, Kluwer Academic Publishers, S. 37 – 47.

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

Gotsopoulou, Niki; Legal Issues on International Franchising and Electronic Commerce, Business Law Review 21 (2); Dec. 2000, Kluwer Academic Publishers, S. 288 – 290.

Berkamp, Lucas; Dekont, Japi, Data Protection in Europe and Internet; An Analysis of The European Community's Privacy Legislation in The Context of The World Wide Web, Electronic Communication Law Review 7 (2/3): 71 – 144; 2000, Kluwer Academic Publishers, S. 71 – 144.

Shaw, Pittman; Potts, Trowbridge, Structuring Technology Outsourcing Relationship; Customer Concerns, Strategies and Process, International Journal of Law and Information Technology, Volume 4, Issue 2; Summer 1996, Oxford University Press, S. 22 - 44

Glatt, C, Comparative Issues in The Formation of Electronic Contracts, International Journal of Law and Information Technology, Volume 6, Issue 1; Spring 1998, Oxford University Press, S. 34 -68.

Lupton, W. Everett, The Digital Signature: Your Identity By The Numbers, The Richmond Journal Of Law and Technology, Volume 6, Issue 2; Fall 1999, S. 22 – 48.

Micheal J. Lookerby, UCITA: The Uniform Computer Information Transaction Act, The Richmond Journal Of Law and Technology, Volume 7, Issue 2; Fall 1999, S. 30 – 45.

Dave Newman; Sathya Rao, Recent Developments Regulatory Aspects of Privacy and Security – A View From Advanced Communication Technologies and Services Programme, Information & Communications Technology Law, Volume 9, Number 2; June 1, 2000. S. 161 – 166

Murray, J, Public Key Infrastructure Digital Signatures and Systematic Risk, The Journal of Information, Law and Technology (JILT), 2003 (1).

Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, Digital Signature Guidelines – Legal Infrastructure For Certification

Authorities and Secure Electronic Commerce, American Bar Association Publishing, Chicago, August 1996.

Greenleaf, Graham; Clarke, Roger, Privacy Implications of Digital Signatures, IBC Conference on Digital Signatures, 12 March 1997, Sydney (http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html Son Erişim: 21/12/2003).

Herrmann, Gerold, Establishing A Legal Framework For Electronic Commerce: The Work Of The United Naitons Commission on International Trade Law (UNCITRAL), International Conference on Electronic Commerce and Intellectual Property, WIPO/EC/CONF/ Geneva, September 1999.

Global Business Dialogue on Electronic Commerce, Brussels Recommendation, Brussels, October 22, 2002.

UNCITRAL, Legal Aspects of Electronic Commerce, Working Group IV (Electronic Commerce) Forty – third Session, New York, 15 -19 March 2004.

ICC, General Usage of International Digitally Ensured Commerce, Paris, 2003.

Albert Gidari, John P. Morgan, Survey of Electronic and Digital Signatures Initiatives in United States, Internet Law & Policy Forum, USA, September 12, 1997.

Chris Kuner, Stewart Baker, Rosa Barcelo, Eric Greenwald, An Analysis of International Electronic and Digital Signature Implementation Initiative, Internet Law & Policy Forum, USA, September, 2000.

Thomas J. Smedinghoff, The Legal Requirements for Creating Secure And Enforceable Electronic Transections, Baker & McKenzie, Illinois, 2002.

Mark Sneddon, Legal Liability and e-Transactions, National Office For The Information Economy, Australia, 2000.

ISTEV, Legal and Regulatory Issues for the European Trusted Services Infrastructure – ETS – Final Report, European Commission, Brussels, 1997.

AICPA/CICA, Privacy Framework, Canada, November 15, 2003 (Revised March 22, 2004).

Baltus/Woop, http://www.edvgt.jura.uni-sb.de/Tagung99/ak99/authentifikation.htm.

Bizer, Johann/Fox, Dirk; " Digital Signierte Zukunft ". Datenschutz und Datensicherheit (DuD) 1997, s. 66.

Boss, Amelia H.; Tearing Down Paper Barriers, Uniform Electronic Act Sets New Contract Rules, LEXIS-NEXIS Academic Universe-Dokument, S. 1-5.

Gerling, Rainer W.; Verschlüsselungsverfahren. Eine Kurzübersicht. Datenschutz und Datensicherheit (DuD) 1997, s. 197-202

Grimm, Rüdiger; Kryptoverfahren und Zertifizierungsinstanzen. Datenschutz und Datensicherheit (DuD) 1996, s. 27-36;

Huhn, Michaela/Pfitzmann, Andreas; Krypto(de)regulierung. Datanschutz-Nachrichten (DANA) 1996, Heft 6, s. 4-13 (İnternet adresi: http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/lit/abstr96.html#HuPf2_96

Keser Berber, Leyla; " İmzalıyorum, O Halde Varım ", Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri, Türkiye Barolar Birliği Dergisi, 2000/2, s. 503-556

Kopp, Wolfgang; Rechtsfragen der Ktyptographie und der digitalen Signatur, http://www.wolfgangkopp.de/krypto.html, s. 1-34.

Königsmann, J.; Elliptische Kurven, http://www.uni-konstanz.de/koenigsmann001.htm.s.1-2.

Köhntopp, Christian; Beweiskraft von PGP-Signaturen, http://www.koehntopp.de.

Ohst, Daniel; Vertrauliche Komunikation, 9.Mai.1996, http://www2.rz.hu-berlin.de.

Özsunay, Ergun; " ELEKRONİK SÖZLEŞMELER - AB Hukuku ile Avusturya ve Alman Hukuklarındaki Gelişmelerin Işığı Altında Türk Hukukuna İlişkin Çözümler - ". AB'de, Bazı Üye Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları - Elektronik Sözleşmeler -" konulu Konfarans'da sunulan Tebliğ, 12 Mayıs 2000, İstanbul (henüz yayımlanmamıştır).

Ramsay, John T.; Digital signatures, A Practitioner's Checklist, s. 1-43.

Rassmann, Steffen; Elektronische Unterschrift im Zahlungsverkehr, CR 1998, s. 36, http://www.mathematik.uni-marburg.de/~cyberlaw/karteikarten/CR_98_36.html, s. 1.

Rossnagel, Alexander; Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung. Datenschutz und Datensicherheit (DuD) 1997, s. 75-81.

Rossnagel, Alexander;, Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung. Datenschutz und Datensicherheit (DuD) 1997, s. 75-81.

Schneier, Bruce; Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in Computer. Almanca tercümesinin 1. Basısı, Bonn 1996;

Seiler, Wolfgang K.; Elliptische Kurven, file://A:\elkurven.htm., s. 1-2.

Timm, Birte; Signaturgesetz und Haftungsrecht. Datenschutz und Datensicherheit (DuD) 1997, s. 525-528.

" Faelschungssicherer unterschreiben ", Fracht und Materialfluss, Mai 1999, s. 43 vd.

" Elektronische Unterschrift ?", Recht im Internet, http://www.mbnet-key.ch/sgnrecht4.htm.

Sicherheit-Die elektronische Unterschrift, http://www.hypowelt.de/info/unterschrift.htm.

Elektronische Unterschrift, http://nestroy.wi-inf.uni-essen.de/Lv/ibis2/folien/07-10.html.

Elektronische Unterschrift für sicheres e-commerce, http://www.seccommerce.de/digitale_signatur.htm.

FVIT Fachverband Informationstechnik, 1998.

Echtheits-Zertifikat, CT, 1998, s. 113.

Verschlüsselung/Codierung/Datenschutz, http://www.glossar.de/glossar/z_verschlussel.htm.

Elektronischer Rechtsverkehr, Digitale Signaturverfahren und Rahmenbedingungen, Bundesnotarkammer (Hrsg.), Köln 1995.

Digitale Unterschrift besiegelt Vertraege, Welt am Sonntag, 1999/1, s. 65 vd.

Chancen und Risiken des Faktors Information – Auswirkungen auf Politik, Gesellschaft, Wirtschaft und Militaer. Forum der Studiengesellschaft der Deutschen Gesellschaft für Wehrtechnik, Bonn-Bad Godesberg, 19-20 November 1997, Kompendium.

Elektronische Unterschrift Kommt (Sicherheit im Internet für rund 150 Mark) (Digitale Signatur soll Hackern ab 1999 das Handwerk legen), http://www.rhein-zeitung.de/on/98/04/27/topnews/esign.html., s. 1-2.

Die elektronische Unterschrift ", Net Investor, 1998/1, s. 15 vd.

SignCard - Technik rund um die Digitale Signatur, http://www.signcard.de/technikçhtm. http://www.europa.eu.int.

SignCard - Technik rund um die Digitale Signatur, http://www.signcard.de/technikçhtm.

WEB ADRESLERİ

http://www.europa.eu.int/comm/internal_market.de/media/sign/composde.htm.

http://www.law.co.il/computer-law/digsig1stdraft.doc.

http://www.mille.com.ar.

http://www.dzsh.de/aktuell/infbrief/97-02/unter.htm.

http://www.telesec.de/recht3.htm.

http://www.ec-guide.com/technologien/16-1-5-2-Signatur.asp.

http://www.teletrust.de/wf/ds.htm.

http://www.rsa.com

http://www.ito.tu-darmstadt./de/Malu/forschung/forschung.html.

http://www.iid.de/rahmen/iukdg.html

http://www.hypovereinsbank.de/?category=/online.../Infos&Page=WasistHBC.

http://www.bmj.bund.de/inhalt/gesetzgebungsvorhaben

http://www.ec-guide.com/technologien/16-1-5-2-Signatur.asp.

EK – 3 : ELEKTRONİK İMZA ULUSAL KOORDİNASYON KURULU HUKUK ÇALIŞMA GRUBU

Başkan:	Yrd.Doç.Dr. Leyla KESER (İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi)
Başkan Yardımcısı:	Yasin BECENİ (Türkekul Hukuk Bürosu)
Kurum Koordinatörü:	Cafer CANBAY (Telekomünikasyon Kurumu)
Raportör(ler):	Tuğrul SEVİM (Türkekul Hukuk Bürosu) Mesut ORTA (Adalet Bakanlığı)
Üyeler:	Doç. Dr. Haluk KONURALP (Ankara Üniversitesi Hukuk Fakültesi) Ali KAYA (Adalet Bakanlığı) Sedat GÜRGEN (Adalet Bakanlığı) Osman Fırat TURAN (Ankara Üniversitesi Rek.) Emel EKEN (Bankacılık Düzenleme ve Denetleme Kurumu) Neslihan YÜKSEK (Bankacılık Düzenleme ve Denetleme Kurumu) Feyza TORLAK (Bankalar Birliği (Yapı Kredi Bank.)) Yrd. Doc. Dr. Leyla KESER (Bilgi Üniversitesi) Ali Aydın SELÇUK (Bilkent Üniversitesi) A.Ramazan ALTINOK (DPT) T.Mete Çanga (DPT) Ali ÇOLAK (Dünya Ticaret Merkezi, Ankara) Engin GİRGİN (Dünya Ticaret Merkezi, Ankara) Sertaç ÇELİKYILMAZ (E-Güven) Can ORHUN (E-Güven/SBS/VeriSign, MPKI) Ahmet HAMZA (EMO)

Sedat BASMAN (EreNet A.Ş.)

Orhan SAMAST (Forsnet Bilgi Teknolojileri)

Yüksel SAMAST (Forsnet Bilgi Teknolojileri)

Işıl KUGAY (İçişleri Bakanlığı)

Özgür AYGÜN (İçişleri Bakanlığı, Sahil Güv. K.lığı)

A. Nurzat TOKER (Maliye Bakanlığı, Bilgi İşlem Dairesi Baş.)

Özlem BENDEN (Maliye Bakanlığı, Bilgi İşlem Dairesi Baş.)

Nezahat AKDENİZ (MSB)

Özlem Özgül YILMAZ (MSB)

Afife AYTAÇ (PTT Genel Müdürlüğü)

Cemil NİŞANKAYA (PTT Genel Müdürlüğü)

H. Handan YAĞIZ (PTT Genel Müdürlüğü)

Mehmet Ali SAKAL (PTT Genel Müdürlüğü)

Nuray KARAGÖZ (PTT Genel Müdürlüğü)

Serdar TEKELİOĞLU (PTT Genel Müdürlüğü)

Aras EROL (Sanayi ve Ticaret Bakanlığı)

Başar KARADENİZ (Sanayi ve Ticaret Bakanlığı)

Bayram KANKAL (Sanayi ve Ticaret Bakanlığı)

Elif SAVAŞ KAPTAN (Sanayi ve Ticaret Bakanlığı)

İlknur ÖZKAZANÇ (Sanayi ve Ticaret Bakanlığı)

Oğuz ŞAHİN (Sanayi ve Ticaret Bakanlığı)

Önder CANPOLAT (Sanayi ve Ticaret Bakanlığı)

Sıddık KAYA (Sanayi ve Ticaret Bakanlığı)

Şakir ENGİN YÜKSEL (Sanayi ve Ticaret Bakanlığı)

Ümit IŞIK (Sanayi ve Ticaret Bakanlığı)

Yusuf ÜSTÜN (Sanayi ve Ticaret Bakanlığı)

Önder ÖZDEMİR (TBD)

Recep USALAN (T.C. Başbakanlık Dış Ticaret Müsteşarlığı)

Bülent ÖZKAN (T.C. Başbakanlık Gümrük Müsteşarlığı)

Bülent TAŞOLUK (T.C. Başbakanlık Gümrük Müsteşarlığı)

Ş. Çiğdem ÇAMURDAN (T.C. Başbakanlık Gümrük Müsteşarlığı)

Birsen ACIR (T.C. Başbakanlık Sermaye Piyasası Kurulu)

Jale ÖZEL (T.C. Merkez Bankası)

Serhat ÖZEREN (TEDER)

Leyla DAYANIR (TOBB)

Mete VARAS (TurSign Dijital Sertifika Hiz. A.Ş.)

Muharrem BÜYÜKBAHÇECİ (TurSign Dijital Sertifika Hiz. A.Ş.)

Cem AKOYMAK (Turkcell)

Burç ONAT (Turkcell)

Rukiye ÖZCİVELEK (TÜBİTAK - BİLTEN)

Saliha KZIILOĞLU (Tüketici Hakları Derneği)

Songül ERCAN (Tüketici Hakları Derneği)

Özgür DANIŞMAN (Tüm İnternet Derneği)

Aslı HELVACIOĞLU (Tüm İnternet Derneği)

Aslıhan ÖZDEMİR (Türk Telekomünikasyon A.Ş.)

Elçin ÇAPANOĞLU (Türk Telekomünikasyon A.Ş.)

Hakan Metin ATİLA (Türk Telekomünikasyon A.Ş.)

Melek AN (Türk Telekomünikasyon A.Ş.)

Erdem TÜRKEKUL (Türkekul Hukuk Bürosu)

Sertan ERATAY (Türkiye Bankalar Birliği)

Attila ÖZGİT (Türkiye Bilişim Derneği)

Önder ÖZDEMİR (Türkiye Bilişim Derneği)

Osman GÜNVER (Türkiye Bilişim Derneği)

Behçet ENVARLI (Türkiye Bilişim Vakfı)

Enis ERYILMAZ (Türkiye İhracatçılar Meclisi (TİM))

Şahin OKTAY (Türkiye İhracatçılar Meclisi (TİM))

Orhan TURAN (Türkiye Noterler Birliği (TNB))

Seden Bolat SIRALİ (TÜSİAD)

Emine YETİM (Ulaştırma Bakanlığı)