1. Elektronik imza, elektronik sertifika, güvenli elektronik imza, nitelikli elektronik sertifika, imza oluşturma verisi, imza doğrulama verisi nedir? Elektronik imza neden ve hangi uygulamalarda kullanılır?

5070 sayılı Elektronik İmza Kanunu'nda tanımlandığı şekliyle;

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

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

Güvenli elektronik imza: Elle atılan imza ile aynı hukukî sonucu doğuran ve Kanun'da belirtilen özel şartları taşıyan elektronik imza

Nitelikli elektronik sertifika: Kanun'da belirtilen koşulları sağlayan, güvenli elektronik imza oluşturmak için sahip olunması gereken elektronik sertifikayı,

İmza oluşturma verisi: İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri, İmza doğrulama verisi: Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri ifade eder. Güvenli elektronik imza, Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri dışında, elle atılan imza yerine, aynı hukuki geçerliliğe sahip olarak, elektronik ortamda imza oluşturmak için kullanılır.

2. Elektronik imzanın faydaları nelerdir? Ne sağlar?

Elektronik imza, elle atılan imzaya eşdeğer nitelikte kullanılabildiği için, elektronik ortamda her türlü resmi işlemin, kağıt ortamına göre daha hızlı, güvenilir ve maliyet etkin biçimde yürütülmesini sağlar. Bu bağlamda elektronik imza, kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik haberleşme ve sözleşmelerde, Kanun kapsamındaki hukuki işlemlerde kullanılabilir.

3. Açık anahtar altyapısı nedir? Neden kullanılır? Ne sağlar?

Açık anahtar altyapısı, elektronik imzanın güvenli ve güvenilir biçimde uygulanmasını sağlamak için kullanılan bir teknolojidir. Açık anahtar altyapısı kullanılarak oluşturulan bir elektronik imzanın kimden geldiğinin belirlenmesi, imzalanmış metnin elektronik ortamdaki doğruluğunun ve bütünlüğünün sağlanması, atılan imzanın imza sahibi tarafından inkar edilememesi sağlanmış olur. Kanun'da yer alan güvenli elektronik imzanın özelliklerinin sağlanması için kullanılır.

4. Zaman damgası nedir? Neden ve hangi uygulamalarda kullanılır?

Zaman damgası Kanun'da "bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt" olarak tanımlanır. Elektronik ortamda doküman, kayıt, sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için kullanılır. Elektronik ortamdaki işlemlere güvenilir zaman bilgisi eklenebilmesini sağlar. Üzerinde zaman bilgisi olması gereken elektronik başvuru, tutanak, sözleşme ve benzeri her türlü elektronik veri üzerinde kullanılabilir.

5. Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) nedir? Görevleri nelerdir?

Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), Kanun'da "elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri" olarak tanımlanır. ESHS'ler, kayıt merkezleri aracılığıyla aldıkları elektronik sertifika başvurularını değerlendirip güvenli koşullar altında işleyerek elektronik sertifikaları üretir, sertifika başvuru sahiplerine ulaştırır. Bunun yanı sıra, sertifika yenileme ve iptal hizmetlerini, sertifika ve iptal durumu yayımlama hizmetlerini ve zaman damgası hizmetlerini verir.

6. ESHS'lerin yükümlülükleri nelerdir? ESHS olmak için hangi özellikleri sağlamak gerekir?

Kanun gereği ESHS'ler;

1. Hizmetin gerektirdiği nitelikte personel istihdam etmekle,
2. Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle,
3. Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle,
4. 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,
5. Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,
6. Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

7. Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,
8. Faaliyetine son vereceği tarihten en az üç ay önce durumu Telekomünikasyon Kurumuna ve elektronik sertifika sahibine bildirmekle yükümlüdür.

ESHS'lerin faaliyete geçebilmesi için güvenli ürün ve sistemleri kullanmak, hizmeti güvenilir bir biçimde yürütmek, sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almakla ilgili şartları sağladığını göstermesi gerekir. ESHS'ler, üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

7. Türkiye'deki ESHS yapısı nasıldır?

Kanun gereği, Türkiye'de elektronik imzanın hukuki ve teknik yönleri ile uygulanmasına ilişkin usul ve esasları düzenleme ve ESHS'lerin faaliyetlerini denetleme görevi Telekomünikasyon Kurumu'na (TK) verilmiştir. Kanun gereği Kurum, gerekli gördüğü zamanlarda ESHS'leri denetleyebilir. Kanundaki şartları yerine getiren gerçek veya özel hukuk tüzel kişileri, TK denetimi sonrası ESHS olarak faaliyete geçebilir. İlgili Başbakanlık genelgesi gereği kamu kurum ve kuruluşları için TÜBİTAK'a bağlı bir sertifikasyon merkezi oluşturulmuştur. Kamu kapsamının dışında kalan sertifika başvuru sahiplerine yönelik olarak, TK denetiminden geçmiş yetkili ESHS'ler elektronik sertifika hizmetleri verirler.

8. Sertifikalar ne kadar süreyle kullanılır? Neden?

Elektronik sertifikaların geçerlilik süreleri güvenlik nedeniyle sınırlandırılmıştır. Geçerlilik süresi sonunda, sertifika sahiplerinin elektronik sertifika kullanımına devam etmek istemeleri halinde sertifikalarını ESHS'lerin bildirecekleri yöntemler uyarınca yenilemeleri gerekir. Nitelikli elektronik sertifikalar için genel olarak 1 (bir), 2 (iki) veya 3 (üç) yıllık geçerlilik süreleri kullanılır.

9. Sunucu (SSL) Sertifikası nedir? Ne sağlar, nelerde kullanılır?

Sunucu (SSL) sertifikaları, İnternet ve her türlü ağ üzerinde istemci bağlantılarını karşılayan sunucuların, bağlanan kullanıcılar tarafından doğrulanması amacıyla kullanılır. Eğer sunucuya bağlanan kullanıcı da elektronik sertifika sahibiyse, sunucu bağlantısı sırasında kullanıcının da kimliğinin doğrulanması mümkündür. Bu tür bir bağlantı sırasında istemci ve sunucu arasında güvenli bir iletişim kanalı oluşturulur ve gönderilip alınan bilgiler şifrelenerek transfer edilir. Sunucu (SSL) sertifikaları, özellikle İnternet üzerinde hizmet veren web sunucularının bağlantı güvenliğinin sağlanması amacıyla kullanılır. Bankacılık, e-ticaret ve e-devlet uygulamaları sunucu (SSL) sertifikalarının sık kullanıldığı alanlardır.

10. Kök sertifika ne demektir?

Bir ESHS'nin, başvuru sahiplerine yönelik olarak sertifika üretebilmesini sağlayan, ürettiği nitelikli elektronik sertifikalar ve sunucu sertifikaları gibi sertifikaları imzalamakta kullandığı imza oluşturma verisine karşılık gelen imza doğrulama verisiyle ESHS'nin kurumsal kimliği arasında bağ kuran, yine ESHS'nin kendi imza oluşturma verisiyle imzalanmış sertifikasına kök sertifika adı verilir. 5070 sayılı Elektronik İmza Kanunu uyarınca TK tarafından yayımlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" gereği, ESHS faaliyete geçmesini müteakip yedi (7) gün içinde; kök sertifikasının sertifika özet değerini ve özetleme algoritmasını kendi İnternet sayfasında yayımlar, ulusal yayın yapan en yüksek tirajlı üç (3) gazetede ilan vermek suretiyle kamuoyuna duyurur ve gazete ilanlarının bir örneğini TK'ya iletir.

11. Elektronik sertifikaların içeriğinde hangi bilgiler vardır?

Elektronik sertifikalarda temel olarak aşağıdaki alanlar bulunur:

1. Sertifika sahibi bilgileri (isim, şirket, çalışılan birim, yer, ülke, e-posta vb.)
2. Sunucu sertifikalarında sunucu bilgileri (alan adı, sunucu adı, şirket adı vb.)
3. Ülke adı TR (Türkiye) olmak üzere ESHS bilgileri
4. Sertifika geçerlilik süresinin başlangıç ve bitiş zamanı
5. Kullanılan elektronik imza oluşturma algoritmaları
6. Sertifika sahibi imza doğrulama verisi
7. Sertifika seri numarası
8. ESHS'nin imzası

Nitelikli elektronik sertifikalarda, Kanun gereği aşağıdaki bilgiler de yer alır:

1. Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare
2. Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi,
3. Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri,
4. Varsa sertifikanın kullanım şartları ve sertifika kullanımına yönelik maddi işlem sınırı.

12. Elektronik imza oluşturma ve doğrulama araçları nedir? Özellikleri ne olmalıdır?

5070 sayılı Elektronik İmza Kanunu'nda tanımlandığı şekliyle;
İmza oluşturma aracı: Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını,
İmza doğrulama aracı: Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını, ifade eder.

Kanun gereği güvenli elektronik imza oluşturma araçları;

1. Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
2. Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
3. Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
4. İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,

sağlayan imza oluşturma araçlarıdır. Güvenli elektronik imza doğrulama araçları ise;

1. İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,
2. İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
3. Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,
4. İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
5. İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,
6. İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

imza doğrulama araçlarıdır.

13. Sertifika iptali, askıya alma, sertifika yenileme, anahtar yenileme nedir? Nasıl yapılır?

Sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda sertifika iptal edilir. Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

1. Sertifika sahibinin talebi,
2. Nitelikli elektronik sertifikaya ilişkin ESHS'de bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması,
3. Sertifika içeriğinde yer alan sertifika sahibi bilgilerinde bir değişiklik olması,
4. Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi,
5. İmza oluşturma verisinin kaybedilmesi, çalınması, ortaya çıkması veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
6. İmza oluşturma verisinin içinde bulunduğu güvenli elektronik imza oluşturma aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
7. Sertifikanın, Sİ ve SUE kitapçıkları ile ESHS Sertifika Sahibi Sözleşmesi hükümlerine aykırı olarak kullanıldığının anlaşılması,
8. ESHS'nin sertifika hizmetleri vermeyi durdurması.

ESHS, elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur. Bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda doğrulama işlemi sonuçlanıncaya kadar, ya da son kullanıcı tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığı zamanlarda gelen talep üzerine, iptal işlemi yapmak yerine ilgili sertifikalar askıya alınır. Askı süresince sertifika üçüncü taraflar tarafından doğrulanamaz durumdadır. Kişisel kullanım amaçlı elektronik sertifikaların, geçerlilik sürelerinin sonunda kullanımına devam edilebilmesi için yenilenmesi gerekir. Sertifika yenileme, sertifikanın süresinin sonunda sertifika bilgilerinde bir değişiklik olmadığı durumlarda yapılır. Sertifika yenileme işlemi sırasında, sertifika sahibinin imza oluşturma ve imza doğrulama veri çifti de yenilenebilir.

14. Konuyla ilgili hukuksal dayanak nedir?

Elektronik imzanın Türkiye'de uygulanmasıyla ilgili hukuki dayanak, "5070 sayılı Elektronik İmza Kanunu" ile TK tarafından yayımlanmış olan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" ve "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" dir.

15. Çapraz Sertifikasyon nedir?

Çapraz sertifikasyon, bir ESHS tarafından üretilen elektronik sertifikaların, diğer bir ESHS'nin ürettiği elektronik sertifikalara güvenen üçüncü taraflar tarafından, ESHS'nin kök sertifikası üçüncü tarafın elinde olmadığı halde doğrulanabilmesini sağlayan, ESHS'lerin birbirlerinin kök sertifikalarını imzalamasıyla oluşturdukları sertifikasyon biçimidir.

16. Yabancı Sertifikalara güvenilebilir mi?

Kanun gereği, yabancı bir ülkede kurulu bir ESHS tarafından verilen elektronik sertifikaların hukukî sonuçları milletlerarası anlaşmalarla belirlenir. Yabancı bir ülkede kurulu bir ESHS tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir ESHS tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılır. Bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki ESHS de sorumludur.

17. Elektronik sertifikalar ne tür yazılımlar ile kullanılabilir?

Elektronik sertifikaların bilgisayar sistemlerine tanıtılması ve elektronik imzalı metinlerin imza doğrulaması için çeşitli istemci yazılımları kullanılabilir. Bu yazılımlar uygulamaya özel geliştirilebileceği gibi, bu işlevi yerine getiren paket programlar da bulunabilir. Pek çok e-posta programı ve İnternet tarayıcısı da elektronik sertifika kullanım özelliklerine sahiptir.

18. Sertifika İlkeleri ve Sertifika Uygulama Esasları nedir? Ne amaçla kullanılır?

Sertifika İlkeleri, sertifika başvurularının alınması, sertifika üretimi ve yönetimi, sertifika yenileme ve iptal işlemleriyle ilgili tüm idari, teknik ve yasal gereklilikleri ortaya koyar; ESHS'nin, sertifika sahibinin ve üçüncü tarafların uygulama sorumluluklarını belirler. Sertifika Uygulama Esasları ise, Sertifika İlkeleri'nde belirlenen gerekliliklere ESHS, sertifika sahipleri ve üçüncü tarafların nasıl uyduğunu, bu gerekliliklerin nasıl hayata geçirildiğini açıklar. ESHS'ler, bağlı bulundukları Sertifika İlkeleri'nin koşullarını, Sertifika Uygulama Esasları uyarınca yürüttükleri işletme faaliyetleriyle sağlar.

19. Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları nedir? Ne amaçla kullanılır?

Zaman Damgası İlkeleri, zaman damgası başvurularının alınması, zaman damgası üretimi ve talep sahibine zaman damgasının gönderilmesi gibi temel zaman damgası hizmet ve işlemleriyle ilgili idari, teknik ve yasal gereklilikleri ortaya koyar; ESHS'nin ve üçüncü tarafların sorumluluklarını belirler. Zaman Damgası Uygulama Esasları ise, Zaman Damgası İlkeleri'nde belirlenen gerekliliklere ESHS ve üçüncü tarafların nasıl uyduğunu, bu gerekliliklerin nasıl hayata geçirildiğini açıklar. ESHS'ler, bağlı bulundukları Zaman Damgası İlkeleri koşullarını, Zaman Damgası Uygulama Esasları uyarınca yürüttükleri işletme faaliyetleriyle sağlar.