BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU
KARARI

Karar Tarihi : 29.05.2019
Karar No : 2019/DK-BTD/160

Gündem Konusu : Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar

KARAR : Bilgi Teknolojileri Dairesi Başkanlığının hazırladığı takrir ve ekleri incelenmiştir.

14.10.2017 tarihli ve 30210 sayılı Resmî Gazete'de yayımlanan e-Yazışma Projesi ile ilgili 2017/21 sayılı Başbakanlık Genelgesi, 15.01.2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu'nun 3'üncü maddesinin birinci fıkrasının (b) bendi ve 02.02.2015 tarihli ve 29255 sayılı Resmi Gazetede yayımlanan Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'in 28'inci maddesi çerçevesinde;

1. Ek'te yer alan "Kamu Kurum ve Kuruluşları Arasında Elektronik Ortamdaki Belge Paylaşımında Kullanılan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Usul ve Esaslar" taslağının onaylanması

hususuna karar verilmiştir.

Bilgi Teknolojileri ve İletişim Kurumundan:

KAMU KURUM VE KURULUŞLARI ARASINDA ELEKTRONİK ORTAMDAKİ BELGE PAYLAŞIMINDA KULLANILAN KURUMSAL ŞİFRELEME ve ELEKTRONİK MÜHÜR SERTİFİKALARINA İLİŞKİN USUL ve ESASLAR

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ile Tanımlar ve Kısaltmalar

Amaç

MADDE 1- (1) Bu usul ve esasların amacı, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında kullanılan kurumsal şifreleme ve elektronik mühür sertifikalarının başvurusunun alınması, oluşturulması, kullanılması, iptali ve yenilenmesi ile ilgili usul ve esasları belirlemektir.

Kapsam

MADDE 2- (1) Bu usul ve esaslar, kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında kullanılan kurumsal şifreleme ve elektronik mühür sertifikalarının başvurusunun alınması, oluşturulması, kullanılması, iptali ve yenilenmesi işlemlerini kapsar.

Dayanak

MADDE 3- (1) Bu usul ve esaslar 02/02/2015 tarihli ve 29255 sayılı Resmi Gazetede yayımlanan Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmeliğin 28'inci maddesine, 14/10/2017 tarihli ve 30210 sayılı Resmî Gazetede yayımlanan e-Yazışma Projesi ile ilgili 2017/21 sayılı Başbakanlık Genelgesine ve 5070 sayılı Elektronik İmza Kanununun 3'üncü maddesinin birinci fıkrasının (b) bendine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4- (1) Bu usul ve esaslarda geçen;

a) Devlet Teşkilatı Merkezi Kayıt Sistemi (DETSİS): Türkiye Cumhuriyeti devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile bunların merkez, taşra ve yurtdışı teşkilatlarında bulunan her düzeydeki birimlerinin hiyerarşik yapıya uygun olarak Türkiye Cumhuriyeti Devlet Teşkilatı Numarası ile tanımlandığı sistemi,
b) Elektronik mühür: Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve elektronik mühür sahibinin kimliğini doğrulama amacıyla kullanılan elektronik veriyi,
c) Elektronik mühür sertifikası: Kamu Sertifikasyon Merkezi tarafından üretilen ve kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında yazışma yapan tarafların kurumsal kimliklerini güvenli bir şekilde tanımlamak ve doğrulamak amacıyla kullanılan elektronik sertifikayı,
ç) Erişim Verisi: Sertifikaya erişim için kullanılan parola, biyometrik değer gibi verileri,
d) ESHS: Elektronik Sertifika Hizmet Sağlayıcısını,
e) E-Yazışma Projesi: Kamu kurum ve kuruluşları arasındaki resmi yazışmaların elektronik ortamda yürütülmesini amaçlayan projeyi,
f) Genelge: 14/10/2017 tarihli ve 30210 sayılı Resmî Gazetede yayımlanan e-Yazışma Projesi ile ilgili 2017/21 sayılı Başbakanlık Genelgesini,
g) İptal Durum Kaydı: Kullanım süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kaydı,
ğ) Kanun: 15/1/2004 tarih ve 5070 sayılı Elektronik İmza Kanunu'nu,
h) Kamu Sertifikasyon Merkezi (Kamu SM): 06/09/2004 tarihli ve 25575 sayılı Resmî Gazetede yayımlanan 2004/21 sayılı Başbakanlık Genelgesi uyarınca Kamu Sertifikasyon Yapısının kurulması ve işletilmesi amacıyla TÜBİTAK BİLGEM bünyesinde oluşturulan ve 30/06/2005 tarihinde Kurum tarafından yetkilendirilen ESHS'yi,
ı) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,
i) Kurul Başkanı: Bilgi Teknolojileri ve İletişim Kurulu Başkanını,
j) Mühür sahibi: Elektronik mührü oluşturan kamu kurumu ve kuruluşunu,

k) Sertifika sahibi: Adına şifreleme sertifikası veya elektronik mühür sertifikası üretilen kamu kurum ve kuruluşunu,
l) Şifreleme: Bir elektronik verinin, kriptografik yöntemler kullanılarak değiştirilmesi suretiyle gizliliğinin sağlanmasına olanak veren tekniği,
m) Şifreleme sertifikası: Kamu SM tarafından üretilen ve kamu kurum ve kuruluşları arasında elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılan açık anahtarı içeren elektronik sertifikayı,
n) Tebliğ: 6/1/2005 tarihli ve 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliği,
o) Teknik Rehber: 02/02/2015 tarihli ve 29255 sayılı Resmi Gazete'de yayımlanan Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'in 3'üncü maddesinin birinci maddesinin (i) fıkrasında tanımlanan e-Yazışma Teknik Rehberini,
ö) TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumunu

ifade eder.

(2) Bu usul ve esaslarda geçen, ancak yukarıda yer almayan tanımlar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM
Şifreleme ve Elektronik Mühür Sertifikalarına İlişkin Hükümler

Şifreleme sertifikası başvurusu ve oluşturulması

MADDE 5 – (1) Kamu kurum ve kuruluşları, elektronik ortamdaki belge paylaşımında kullanmak üzere şifreleme sertifikası almak amacıyla Kamu SM'ye başvuruda bulunur.

(2) Kamu SM, başvuru yapan tarafın şifreleme sertifikası almaya yetkili olup olmadığını DETSİS vasıtasıyla teyit eder.
a) Kamu SM, DETSİS'te bilgileri bulunmayan veya şifreleme sertifikası almaya yetkili olmayan tarafın başvurusunu reddeder.
b) Kamu SM, DETSİS'te bilgileri bulunan ve şifreleme sertifikası almaya yetkili taraflara Kanun ve ilgili mevzuat ile belirlenen teknik kriterlere uygun olarak şifreleme sertifikasını üretir ve DETSİS'e aktarır. Kamu SM, şifre çözme amacıyla eş zamanlı ürettiği kriptografik özel anahtarı ilgili Kuruma güvenli bir şekilde teslim eder.
c) Kamu SM, şifreleme sertifikalarıyla ilişkili olarak ürettiği kriptografik özel anahtarı sisteminde saklayamaz.

(3) Başvurunun Kamu SM'ye ulaşmasının ardından en fazla 15 (on beş) iş günü içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

(4) Şifreleme sertifikası, geçerlilik süresi en fazla 1(bir) yıl olacak şekilde Kamu SM tarafından, Tebliğ'in 6 ncı maddesinin (b) fıkrasında imza oluşturma ve doğrulama verileri için belirlenen kriterlere uygun olarak üretilir.

(5) Şifreleme sertifikası Kamu SM tarafından, ITU X.509 ve RFC 5280 standartlarına uygun olarak üretilecektir. Bu kapsamda;
a) "Özne (Subject) Alanı", "*CommonName*" niteliğine ilgili kamu kurumu veya kuruluşunun tümü büyük harf olacak şekilde DETSİS'te kayıtlı ünvanı,
b) "Özne (Subject) Alanı", "*SerialNumber*" niteliğine ilgili kamu kurumu veya kuruluşunun DETSİS'te kayıtlı tekil kayıt numarası,
c) "Özne (Subject) Alanı", "*Country*" niteliğine *"TR"* ibaresi,
ç) "Kullanım Kısıtı" şifreleme sertifikasının kısıtına ilişkin "*Bu sertifika, 2017/21 sayılı Başbakanlık Genelgesi kapsamında sadece şifreleme amacıyla kullanılır."* ibaresi,
d) "Anahtar Kullanımı (Key Usage)", *"KeyUsage"* eklentisine *"keyEncipherment"* ibaresi,
e) "Genişletilmiş Anahtar Kullanımı (Extended Key Usage)", "ExtendedKeyUsage" eklentisine Kamu SM tarafından belirlenen kurumsal şifreleme sertifikası nesne belirteci

yazılarak üretilir.

Şifreleme sertifikasının kullanılması

MADDE 6 – (1) Kamu kurum ve kuruluşları;

a) Şifreleme sertifikası ile şifreleme sürecini Genelge ve Teknik Rehberde tanımlanmış süreç ve teknik kriterlere uygun olarak yürütür.
b) Şifreleme sertifikasının sadece elektronik ortamdaki belge paylaşımında şifreleme yapmak amacıyla kullanılmasını sağlar ve bu kapsamda gerekli önlemleri alır. Şifreleme sertifikalarının bilgi ve belgelerin şifrelenerek uzun süreli saklanması ve imzalama gibi amaçlarla kullanılmasını engeller.

(2) Kurumların şifreleme sertifikaları DETSİS web servisleri üzerinden kamu kurum ve kuruluşları ile paylaşılabilir.

Elektronik mühür sertifikası başvurusu ve oluşturulması

MADDE 7– (1) Kamu kurum ve kuruluşları, elektronik ortamdaki belge paylaşımında kullanmak üzere elektronik mühür sertifikası almak amacıyla Kamu SM'ye resmi yazıyla başvuruda bulunur.

(2) Kamu SM, başvuru yapan tarafın elektronik mühür sertifikası almaya yetkili olup olmadığını DETSİS vasıtasıyla teyit eder.
a) Kamu SM, DETSİS'te bilgileri bulunmayan veya elektronik mühür sertifikası almaya yetkisi olmadığı belirtilen tarafın başvurusunu reddeder.
b) Kamu SM, DETSİS'te bilgileri bulunan ve elektronik mühür sertifikası alma yetkisi olduğu belirtilen taraflara Kanun ve ilgili mevzuat ile belirlenen teknik kriterlere uygun olarak elektronik mühür sertifikasını üretir ve başvuru yapan tarafa teslim eder.

(3) Başvuruya ilişkin belgelerin Kamu SM'nin eline geçmesinin ardından en fazla 15 (on beş) iş günü içinde sertifika başvurusu işleme alınır ve sonuçlandırılır.

(4) Elektronik mühür sertifikası geçerlilik süresi en fazla 1(bir) yıl olacak şekilde Kamu SM tarafından, Tebliğ'in 6 ncı maddesinin (b) fıkrasında imza oluşturma ve doğrulama verileri için belirlenen kriterlere uygun olarak üretilir.

(5) Elektronik mühür sertifikası Kamu SM tarafından, 18/4/2007 tarihli ve 2007/DK-77/207 sayılı Kurul Kararı ile yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri" dokümanına uygun olarak ve bu profil dokümanına göre;
a) "Özne (Subject) Alanı" başlıklı 4.1.4 maddesindeki "*CommonName*" niteliğine ilgili kamu kurumu veya kuruluşunun tümü büyük harf olacak şekilde DETSİS'te kayıtlı ünvanı yazılarak,
b) "Özne (Subject) Alanı" başlıklı 4.1.4 maddesindeki "*SerialNumber*" niteliğine ilgili kamu kurumu veya kuruluşunun DETSİS'te kayıtlı tekil kayıt numarası yazılarak,
c) "Özne (Subject) Alanı" başlıklı 4.1.4 maddesindeki "*Country*" niteliğine *"TR"* ibaresi yazılarak,
ç) "Kullanım Kısıtı" başlıklı 4.2.8.4 maddesinde şifreleme sertifikasının kısıtına ilişkin "*Bu sertifika, elektronik mühürleme amacıyla kullanılır."* ibaresi yazılarak,
d) "Anahtar Kullanımı (Key Usage)" başlıklı 4.2.2. maddesindeki *"KeyUsage"* eklentisine *"digitalSignature"* ve "*nonRepudiation*" ibaresi yazılarak,
e) "Genişletilmiş Anahtar Kullanımı (Extended Key Usage)" başlıklı 4.2.5. maddesindeki *"ExtendedKeyUsage"* eklentisi bulunmadan

üretilir.

Elektronik mühür sertifikasının kullanılması

MADDE 8 – (1) Kamu kurum ve kuruluşları;
a) Elektronik mühür sertifikasının kullanımını Genelge ve Teknik Rehberde tanımlanmış süreç ve teknik kriterlere uygun olarak yürütür.
b) Elektronik mühür sertifikasının şifreleme amacıyla kullanılmaması için gerekli tedbirleri alır.

Şifreleme ve elektronik mühür sertifikalarının yenilenmesi

MADDE 9– (1) Şifreleme ve elektronik mühür sertifikalarının geçerlilik süresinin sona ermesinden önce sertifika sahibi yenileme talebini Kamu SM'ye iletir.

(2) Sertifika sahibinin talebi doğrultusunda şifreleme veya elektronik mühür sertifikası Kamu SM tarafından sertifikanın ilk üretim süresi ile aynı sürede olacak şekilde yenilenir.

(3) Şifreleme veya elektronik mühür sertifikasına ilişkin bilgilerde değişiklik meydana gelmesi hâlinde ilgili kamu kurum ve kuruluşu KamuSM'yi bilgilendirir.

(4) Kamu SM, şifreleme veya elektronik mühür sertifikasını, sertifika sahibine ait bilgilerin geçerliliğini doğrulayarak yeniler ve buna ilişkin olarak DETSİS'te gerekli güncellemeleri yapar.

Şifreleme ve elektronik mühür sertifikalarının iptal edilmesi

MADDE 10– (1) Şifreleme veya elektronik mühür sertifikasının güvenliğine ilişkin tehdit oluşması, erişim verisinin yetkisiz ele geçirilmesi veya unutulması, sertifikada bilgi değişikliği gerekmesi, sertifika sahibinin talebi gibi durumlarda sertifika Kamu SM tarafından iptal edilir, sertifika sahibi bilgilendirilir ve eşzamanlı olarak DETSİS'e bildirilir.

(2) Şifreleme ve elektronik mühür sertifikası iptal talebi; Kamu SM, sertifika sahibi kamu kurum veya kuruluşu ve sözleşme ile belirlenen kişiler tarafından yapılabilir.

(3) İptal talebinin alınmasını müteakip şifreleme veya elektronik mühür sertifikası derhal iptal edilir. İptal edilen şifreleme veya elektronik mühür sertifikası, geçerlilik süresi sonuna kadar iptal durum kayıtlarında yer alır.

(4) Kamu SM, şifreleme ve elektronik mühür sertifikalarına ilişkin iptal durum kayıtlarını ücretsiz ve kesintisiz olarak kamu erişimine açık tutar.

(5) Şifreleme ve elektronik mühür sertifikaları geçmişe yönelik iptal edilmez.

Genel hükümler

MADDE 11- (1) Şifreleme ve elektronik mühür sertifikalarına sahip olacak kamu kurum ve kuruluşlarının belirlenmesinde DETSİS'ten sorumlu birim yetkilidir.

(2) Şifreleme ve elektronik mühür sertifika başvurularının alınması, oluşturulması, yenilenmesi, iptal edilmesi ve yaşam döngüsünün yönetiminde, nitelikli elektronik sertifikalar ile şifreleme ve elektronik mühür sertifikaları arasındaki yapısal ve işlevsel farklılıklar nedeniyle uygulanamayan hususlar dışında, Kanun ve ilgili ikincil düzenlemelerde nitelikli elektronik sertifikalar için tanımlanmış süreç ve teknik kriterlere uyulması esastır.

(3) Kamu SM, şifreleme ve elektronik mühür sertifikalarını, Tebliğ'in 11'inci maddesinin birinci fıkrasının (b) bendinin (i) ve (iii) alt bentlerinde belirlenen standartlara uygun güvenli elektronik imza oluşturma araçlarından birine yükleyerek ilgili kuruma teslim eder. İşbu maddede belirlenen standartlara uygun milli veya yerli güvenli elektronik imza oluşturma aracı mevcut ise bu cihazın tercih edilmesi esastır.

(4) Şifreleme ve elektronik mühür sertifika başvurularının alınması, oluşturulması, yenilenmesi, iptal edilmesi gibi işlemler Kanun ve ilgili mevzuat kapsamında; ilgili kamu kurumu veya kuruluşu ile Kamu SM arasında akdedilen sözleşme veya taahhütname gibi yöntemlerle yapılır.

ÜÇÜNCÜ BÖLÜM
Son Hükümler

Yürürlük

MADDE 12- (1) Bu Usul ve Esaslar Kurul tarafından kabul edildiği tarihte yürürlüğe girer.

Yürütme

MADDE 13- (1) Bu Usul ve Esas hükümlerini Kurul Başkanı yürütür.