e-tuğra

NİTELİKLİ ELEKTRONİK SERTİFİKA İLKELERİ

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
Sürüm:6.0
Yürürlük Tarihi: Şubat, 2022
Güncelleme Tarihi: 14/02/2022

Ceyhun Atıf Kansu Cad. 130/58
Balgat / ANKARA
TURKİYE

Tel: 90.850.532.23.14
Tel: 90.850.532.23.12
Faks: 90.312.473.56.91

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. **Nitelikli Elektronik Sertifika İlkeleri**

Açıklamalar ve Uyarılar

İÇERİK

DOKUMAN GEÇMİŞİ

Sürüm	Yayın Tarihi	Yayınlayan(lar))	Açıklama
V4.0	20/06/2016		Format Değişikliği
V4.1	26/08/2016		Yıllık Yönetim Gözden Geçirme
V4.2	29/09/2017		Yıllık Yönetim Gözden Geçirme
V4.3	26/01/2018		ETSI 319-411x Entegrasyonu Yıllık Yönetim Gözden Geçirme
V 4.4	29/08/2018		Yıllık Yönetim Gözden Geçirme. Kök Bilgileri Eklendi.
V 4.5	21/10/2019		Bayiler/Satıcılar eklendi Sertifika Ağacı Eklendi CabForum doküman versiyonları Sertifika başvuruları bölge kısıtlamaları ve Sertifika Zincirleri Eklendi.
V 4.6	30/03/2020		Yeni Köklerin Eklenmesi Yıllık Yönetim Gözden Geçirme
V 4.7	12/03/2021		İptal Süreçleri düzenlendi İptal kontak bilgisi eklendi Alt Kök kullanım alanları BR Gereksinimleri kontrolleri yapıldı
V4.8	05/07/2021		Özel anahtar güvenliği için Mozilla 2.7.1 güncellemelerini bölüm 4.9.12'de sunmak. Alan Adlarının Kimlik Doğrulamasına İlişkin Revizyon Yaşam Döngüsü Teknik Kontrollerinde Revizyon
V 4.9	20/08/2021		Uyumluluk dökümanları sürümleri ve sertifika profilleri güncellendi.
V 5.0	25/10/2021		Uyumluluk kontrolleri
V 5.1	10/01/2022		Yıllık Yönetim Gözden Geçirme
V 6.0	28/01/2022		SSL ve KIS hizmetlerinin SUE ve Sİ dokümanlarının Türkçe versiyonun undan çıkarılması çıkarılması bu dokümanların Türkçe versiyonun sadece NES'leri kapsayacak şekilde düzenlenmesi ve adının Nitelikli Elektronik Sertifika İlkeleri (NESİ) olarak ilgili Sertifika Uygulama Esasları Dokümanın da aynı şekilde Nitelikli Elektronik Sertifika Uygulama Esasları NESUE olarak değiştirilmesi.

1. GİRİŞ

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (bundan sonra "e-tuğra" olarak anılacaktır.) Türk Ticaret Kanunu hükümleri uyarınca kurularak faaliyetlerini sürdüren bir anonim şirkettir. "e-tuğra", 5070 sayılı Elektronik İmza Kanunu'nun 8. Maddesi hükmü uyarınca Bilgi Teknolojileri ve İletişim Kurumu'na usulü dairesinde bildirimde bulunarak ve kanuni gereklilikleri yerine getirerek Elektronik Sertifika Hizmet Sağlayıcı (Kısaca "ESHS") sıfatıyla elektronik imza, elektronik sertifika ve zaman damgası ile ilgili hizmetleri sunma hak ve yetkisini elde etmiştir.

Nitelikli Elektronik Sertifika İlkeleri (Kısaca "NESİ" veya "Sİ") olarak isimlendirilen bu doküman "e-tuğra"nın "ESHS" sıfatıyla yürüttüğü faaliyetler sırasında yerine getirdiği teknik ve hukuki gereklilikleri, "ESHS"nin faaliyetlerini, teknik ve organizasyon altyapısını, "ESHS"nin sunduğu hizmetlere ilişkin süreçlerde belirli roller üstlenen tarafların sorumluluklarını açıklamak ve kamuoyuna duyurmak üzere hazırlanmıştır.

Bu doküman sadece Nitelikli Elektronik Sertifika ("NES") hizmetleri kapsamında olup, diğer Sertifika Hizmetleri (SSL, KIS, vb.) kapsam dışıdır ve ilgili süreçleri farklı Uygulama Esasları dökümanları içerisinde yürütülür. Bundan sonra "Sertifika" deyiminden kasıt aksi belirtilmedikçe Nitelikli Elektronik Sertifikayı ("NES") kasteder.

Bu doküman, sertifika başvurularının alınması, üretimi ve yönetimi, sertifika yenileme ve sertifika iptal işlemleriyle ilgili hizmetlerin, idari, teknik ve yasal gerekliliklere uygun olarak yürütülmesiyle ilgili ilkeleri ortaya koyar; elektronik sertifika hizmet sağlayıcısı (ESHS) olarak "e-tuğra"nın, sertifika sahibinin ve üçüncü kişilerin uygulama sorumluluklarını belirler

"e-tuğra"nın elektronik sertifika hizmet sağlayıcılığı alanındaki faaliyetlerini nasıl yürüttüğünü göstermek amacıyla;

- 5070 sayılı Elektronik İmza Kanunu (Kısaca "Kanun"), Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (Kısaca "Yönetmelik") ile Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (Kısaca "Tebliğ") uyarınca ETSI TS 101 456, IETF RFC 3647 standartlarına ile CWA 14167-2, CWA 14167-3 veya CWA 14167-4 standartlarına ve
- "NES" Dışında Diğer Sertifikaları için ETSI EN 319 411-1 ve ilgili ETSI EN 319 401 standartlarına uygun hazırlanmıştır.

Bu dokümanlardan herhangi biri ile bu doküman arasında bir uyuşmazlık olması durumunda, Tebliğ veya ETSI dokümanları dikkate alınır.

1.1. Genel

"e-tuğra", "Kanun" ve ilgili mevzuattaki gereklilikleri yerine getirerek Bilgi Teknolojileri ve İletişim Kurumu'na usulü dairesinde bildirimde bulunmuş ve bildirimde belirttiği koşulları sağladığı "Bilgi Teknolojileri ve İletişim Kurumu tarafından uygun görülerek faaliyete geçmesi hususunda yetki verilmiş bir "Elektronik Sertifika Hizmet Sağlayıcısı" dır.

“e-tuğra”, kendisi tarafından oluşturulan elektronik sertifikaların özelliklerini ve kullanımına ilişkin hususları, sertifikasyon sürecini, sertifikasyon sürecine katılan tarafların hak ve yükümlülüklerini, "ESHS" olarak yürüttüğü teknik ve operasyonel faaliyetlerini Sertifika İlkeleri (“Sİ”) dokümanında kamuoyuna ve ilgili taraflara yayınlar. “e-tuğra” işletme faaliyetlerini, elektronik sertifika hizmet sağlayıcısı olarak, bu Sertifika İlkeleri (“Sİ”) kitapçığı hükümlerine bağlı bir uygulama kitapçığı olan bu ilgili sertifika uygulama esasları (“SUE”) uyarınca yürütür ve kamuoyunun ve ilgili tarafların bilgisine sunar. Bu dokümanda yer alan ilkeler, “e-tuğra”nın tüm müşteri hizmetleri, kayıt birimlerini ve sertifika üretim uygulamalarını yani “e-tuğra”nın verdiği tüm elektronik sertifika hizmetlerini kapsar.

1.2. Kitapçık Adı ve Tanımlama

Bu “Sİ” dokümanı, “e-tuğra” Sertifika İlkeleri açıklamak ve tanımlamak amacıyla hazırlanmış olup, adı “e-tuğra Sİ dokümanı”dır. Kitapçığın sürüm numarası ve tarihi kapak sayfasında yer almaktadır.

“e-tuğra Sİ dokümanı”, kapsadığı sertifika ilkeleri Türk Standartları Enstitüsün’nden (“TSE”)’den alınan “2.16.792.3.0.4” belirteçleri (OID) kullanılarak aşağıda verilen tüm sertifika ilkelerini kapsamaktadır:

Bu “Sİ” dokümanı http://www.e-tugra.com.tr adresinde kamuya açık olarak yayınlanır.

“e-tuğra” Nitelikli Elektronik Sertifika İlkeleri
5070 sayılı Kanun ile ilgili yönetmelik ve tebliğ uyarınca, bireylerin elle atılan imzaya eşdeğer güvenli elektronik imza kullanımına olanak veren nitelikli elektronik sertifikaları kapsar.
Nesne Belirteci: 2.16.792.3.0.4.1.1.1

1.3. Katılımcılar

“e-tuğra” Sİ ve SUE dokümanları kapsamında tanımlanan katılımcılar “e-tuğra”nın “ESHS” işleyişinde rol alan, işleyişle ilgili hak ve yükümlülükleri bulunan taraflardır.

“e-tuğra” Sİ ve SUE dokümanları kapsamında katılımcılar, Elektronik Sertifika Hizmet Sağlayıcısı - "ESHS" (“e-tuğra”), Kayıt Birimleri, Sertifika Sahipleri ve Üçüncü Kişilerdir.

1.3.1. Elektronik Sertifika Hizmet Sağlayıcısı (“e-tuğra”)

“e-tuğra”, “ESHS” işleyişi içerisinde 5070 sayılı Elektronik İmza Kanunu ve ilgili mevzuat hükümleri ile bu döküman doğrultusunda hak ve yükümlülükleri belirlenmiş olan bir “ESHS”dir. “e-tuğra” sertifika istekleri alınması, üretilmesi, yayınlanması, iptal ve sertifika yenilenmesi, düzenlenmesi, “SİL” ve “ÇSDP” hizmetlerinin gerçekleştirilmesi gibi Açık Anahtar Altyapısı operasyonları ile ilişkili işlevleri gerçekleştirir. Tüm bu operasyonlar ve işlevler “e-tuğra” merkezinde bulunan “Güven Merkezi” tarafından gerçekleştirilir.

“e-tuğra” tarafından oluşturulan son kullanıcı sertifikaları, “e-tuğra” alt kök sertifikalar tarafından imzalanır;

“e-tuğra” “ESHS” alt kök sertifikaları da, sertifika türüne göre, sertifika kullanım amaçlarına göre oluşturulur “e-tuğra” kök sertifikası tarafından imzalanır.

1.3.2. Kayıt Birimleri

Kayıt Birimleri (Kısaca “KB”), sertifika başvurusu, iptal ve yenileme gibi son kullanıcıya yönelik ilgili hizmetleri yürüten, doğrudan “e-tuğra”nın kontrol ve denetimi altında olan yerleşik yapılar ve bu yerleşik yapılar içerisinde istihdam edilen ve/veya ettirilen “e-tuğra”ya bağlı personel veya “e-tuğra” ile Yetkili Kayıt Birimi Sözleşmesi yapmış olan gerçek ve/veya tüzel kişilerdir.

"KB"ler "e-tuğra" tarafından belirlenen belgelere dayanarak, Sertifika talebinde bulunan kişilerin kimliklerini ve/veya ünvanlarını tanımlama ve doğrulama işlemleri ile sertifika içerisinde yer alacak bilgilerin geçerliliğini kontrol ederler. "KB"ler bunun yanında "Sertifika Sahipleri" ile "e-tuğra" arasında sertifikanın yaşam zinciri süresince yürütülecek olan işlemlere ilişkin başvuruların alınması ve gerekli olan operasyonların "e-tuğra" adı ve hesabına yürütülmesi noktasında sorumluluk üstlenebilirler.

"KB"ler aracılığıyla yapılacak sertifika başvuruları, başvuru sahibinin "KB" ofisine bizzat gelerek yüz yüze başvuruda bulunması; gerekli bilgi ve belgeleri "KB" ofisi yetkilisine teslim etmesi veya gerekli bilgi ve belgeleri uzaktan başvuru prosedürleri doğrultusunda "KB" ofisine posta ile yollanması esasına dayanmaktadır. Her iki durumda da, sertifika talepleri "e-tuğra" "Güven Merkezi"ne iletilir ve sertifika üretimi gerçekleştirilir.

"KB"ler ayrıca "NES" sahiplerine asgari güvenli elektronik imza oluşturma aracı ve "NES"den oluşan ancak bunlarla sınırlı kalmamak üzere "e-tuğra"nın yürüttüğü faaliyetlere ilişkin çeşitli ekipman ve hizmetlerin de içerisinde yer alabileceği "güvenli e-imza paketi"ne ilişkin başvuru işlemlerinin de "e-tuğra" adı ve hesabına yürütülmesini de sağlarlar. Gerekli güvenlik önlemlerine sahip "KB"ler, "tüm onayları tamamlanmış nitelikli elektronik sertifika başvuruları için güvenli elektronik imza oluşturma işlevini de yerine getirebilirler.

"e-tuğra", "KB" ofislerinin adreslerini ve iletişim bilgilerini "e-tuğra" web sitesi aracılığıyla kamuoyuna duyurur.

1.3.3. Sertifika Sahipleri

Kimlik veya unvanları doğrulanan ve buna bağlı olarak adlarına sertifika üretilen kişi veya kurumlar sertifika sahibidir.

Kimlik ve/veya unvan doğrulaması, başvuru yapılan sertifika türüne göre ilgili mevzuat ve standartlara göre yapılır.

Sertifika sahibinin sorumluluğu ve sertifika kullanımından doğan sonuçlar, başvuru yapılan sertifika türüne göre ilgili mevzuatla ve sertifika sahibi tarafından imzalanan taahhütname veya sözleşmeyle belirlenir.

5070 sayılı Elektronik İmza Kanunu'na göre "NES"ler sadece gerçek kişiler adına "ESHS"ler tarafından oluşturulabilir. "NES" sahibi "e-tuğra" tarafından kamuoyuna açıklanan "NESUE", "NESİ", "NES" Sahibi ile akdedilen "NES Kullanıcı Sözleşmesi" ve "e-tuğra" tarafından belirlenen gereklilikleri yerine getirerek adına "NES" oluşturulmuş gerçek kişilerdir.

1.3.4. Bayiler/Satıcılar

Bayiler belirli bir hak ve bölge kısıtlaması olan ve sadece e-tuğra sertifikalarının pazarlanmasından ve satışından sorumludur. Bayiler aracılığıyla yapılan tüm sertifika başvuruları e-tuğra veya e-tuğra Kayıt Yetkilileri tarafından onaylanır ve işlenir. Tüm alt kökler için başvuruların doğrulanması ve sertifikaların oluşturulması sadece e-tuğra tarafından yapılır.

1.3.5. Üçüncü Kişiler

Üçüncü kişiler, "e-tuğra" tarafından verilmiş olan sertifikalara bağlı imza oluşturma verileriyle imzalanmış belgeleri alan, ilgili sertifikalara güvenen taraflardır.

Sertifika sahipleri yukarıda bahsedilen doğrulama süreçlerini kendileri yerine getirmeleri durumunda üçüncü kişi olarak hareket etmektedirler.

1.3.6. Diğer Katılımcılar

"e-tuğra"nın verdiği sertifika hizmetleri kapsamında sertifika üretimi, bilgi deposu yayımlama ve sertifika bilgilerinin güvenliğinin sağlanması gibi işlemlerin tümü bizzat kendisi tarafından gerçekleştirilir.

Diğer katılımcılar "e-tuğra"nın, sertifika hizmetlerini gerçekleştirirken iş birliği yaptığı ve hizmet aldığı tüm gerçek/tüzel kişiler ve kuruluşlardır.

"e-tuğra" diğer katılımcılar ile verecekleri hizmetlerin güvenilir ve doğru biçimde verilmesi, iş süreçlerin "e- Tuğra" tarafından "Sİ" ve "SUE"ye göre hazırlanmış prosedür ve talimatlara uygun olarak yerine getirilmesi, ve müşterilerle ilgili gizli veya özel bilgilerin gizli kalacağının garanti edilmesi amacıyla sözleşmeler imzalar.

1.4. Sertifika Kullanımı

1.4.1. Geçerli Sertifika Kullanım Şekilleri

"e-tuğra" kök ve alt kök sertifikaları sadece kullanım amaçları doğrultusunda sertifika imzalanması ile bahsi geçen sertifikaların ve verilerin doğrulanması süreçlerinde kullanılabilir.

"e-tuğra" tarafından oluşturulan "NES"ler sadece güvenli elektronik imza oluşturma ve doğrulama süreçleri içerisinde, "NES"in içinde yer alan kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde ve "NES Kullanıcı Sözleşmesi" hükümlerine uygun olarak kullanılabilirler. E-devlet, e-ticaret ve benzeri uygulamalarda belge, doküman ve form imzalamak, elektronik ortamdaki her türlü ticari veya resmi evrak ve dokümanları imzalamak, kimlik tanımlama ve doğrulama gerektiren ağ ortamlarında kimliği ispat etmek geçerli sertifika kullanım şekilleridir. "NES"ler aynı zamanda üçüncü kişiler tarafından "NES"in geçerliliğinin doğrulanması ve "NES" içeriğine erişilmesi amaçlarıyla da kullanılabilirler.

Tüm sertifikaların kullanım hakları sadece sertifika sahiplerine aittir.

1.4.2. Yasaklanan Sertifika Kullanım Şekilleri

"e-tuğra" tarafından oluşturulan kök ve alt kök sertifikalarının kullanım alanları dışında kullanılmaları yasaktır.

"e-tuğra" tarafından oluşturulan "NES"ler Elektronik İmza Kanunu'nunda kısıtlanan işlemlere ilişkin güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanılması yasaktır. "NES"ler mevzuatta belirlenen şartlar dışında kullanılamaz.

Diğer "e-tuğra" sertifikalarının kullanım hakları sadece sertifika sahiplerine aittir, sertifika sahiplerinin uhdesi dışında kullanılmaları yasaktır.

Tüm Sertifikalar, işbu dokümanda belirtilen amaçlar ve sınırlar dışında kullanılamaz.

1.4.3. Sertifika Hiyerarşisi

Aşağıda Kök Sertifikalar ve bu Kök CA'lar tarafından verilen Alt Kökler bu belgedeki politikalara tabidir.

1.4.3.1 Kök Sertifikalar ve Alt Kök Sertifikalar

Kök Sertifika Tanımı	E-Tugra Certification Authority

Kök Sertifika Konu	CN=E-Tugra Certification Authority, OU=E-Tugra Sertifikasyon Merkezi, O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., L=Ankara, C=TR
SHA-256 parmak izi	B0:BF:D5:2B:B0:D7:D9:BD:92:BF:5D:4D:C1:3D:A2:55:C0:2C:54:2F:37:83:65:EA:89:39:11:F5:5E:55:F2:3C
Sertifika Seri Numarası	6A683E9C519BCB53

Tanımı	**Sertifika Konu**	**SHA-256 parmak izi**	**Seri Numarası**	**Kullanım Amacı**
E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı v2 OU = E-Tuğra Sertifikasyon Merkezi O = E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. L = Ankara C = TR	DD:2C:B2:EE:C5:2F:5E:96:AB:1C:B8:43:09:52:FB:56:C8:E6:AB:DF:F2:1E:AC:D7:68:4B:1C:D7:38:AA:CC:FF	1F0EC403B3801CAD	- (Nitelikli Elektronik İmza için) 19 Ocak 2022 tarihinde Kullanımı Durdurulmuştur.

Kök Sertifika Tanımı	E-Tugra Certification Authority Root NES RSA v3
Kök Sertifika Konu	CN = E-Tugra Certification Authority Root NES RSA v3 OU = E-Tugra Sertifikasyon Merkezi O = E-Tugra EBG A.S. L = Ankara C = TR
SHA-256 parmak izi	F0:72:2F:1B:0B:A2:DA:29:C6:A7:EE:AF:91:20:54:C5:56:C6:06:AC:1B:95:B7:45:32:AC:7F:81:B9:2D:F6:9E
Sertifika Seri Numarası	40:5B:DE:ED:02:03:E8:D7:AC:6E:53:A1:0E:5B:EF:A5:33:C7:4E:92

Tanımı	**Sertifika Konu**	**SHA-256 parmak izi**	**Seri Numarası**	**Kullanım Amacı**
E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı RSA v3	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı RSA v3,OU=E-Tuğra Sertifikasyon Merkezi,O=E-Tuğra EBG A.Ş.,L=Ankara,C=TR	24:72:5D:37:5D:59:0B:83:6F:B4:36:B8:81:10:57:6E:3F:D9:26:26:47:7E:EF:36:EC:D6:E0:EB:68:53:6D:68	30:F8:23:9C:14:F1:D9:9E:03:3E:CC:DB:70:F9:F2:C7:38:11:15:EA	- (Nitelikli Elektronik İmza için)

Kök Sertifika Tanımı	E-Tugra Certification Authority Root NES ECC v3
Kök Sertifika Konu	CN = E-Tugra Certification Authority Root NES ECC v3 OU = E-Tugra Sertifikasyon Merkezi O = E-Tugra EBG A.S. L = Ankara C = TR
SHA-256 parmak izi	1C:B8:DF:3E:F2:44:B4:7C:BB:99:CC:5D:A8:26:B1:BD:67:34:59:F2:2C:B7:84:D2:3C:70:C9:5E:67:72:CF:D4
Sertifika Seri Numarası	62:8D:9B:69:79:D1:64:83:6D:FF:C8:27:AE:42:6D:92:6A:50:DF:94

Tanımı	**Sertifika Konu**	**SHA-256 parmakizi**	**Seri Numarası**	**Kullanım Amacı**
E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı ECC v3	CN = E-Tuğra Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı ECC v3,OU = E-Tuğra Sertifikasyon Merkezi,O = E-Tuğra EBG A.Ş.,L = Ankara,C = TR	93:0B:9C:7E:43:17:EC:1D:43:6A:64:EB:32:C5:54:AE:B2:86:FC:60:49:B2:F2:33:D6:60:7F:64:15:28:A0:2A	5C:0B:72:EC:33:AC:6F:B9:0A:28:EB:06:1D:3F:DC:16:D4:21:46:66	- (Nitelikli Elektronik İmza için)

1.5. Sertifika İlkeleri Yönetimi

"SUE" dokümanının bağlı bulunduğu "Sİ" dokümanının yönetiminden, sertifika ilkelerini oluşturan otorite olarak, "e-tuğra" sorumludur.

1.5.1. "e-tuğra Sİ dokümanı" ile ilgili Yetkili Kurum

"e-tuğra Sİ dokümanı"ın yayınlanmasından, değiştirilmesinden, yenilenmesinden ve bu dokümana ilişkin diğer tüm işlemlerden "e-tuğra" tarafından bu hususla ilgili yetkilendirilmiş "e-tuğra" personelinin oluşturduğu güvenlik forumu sorumludur. İşbu dokümanın tüm hakları "e-tuğra"ya aittir.

1.5.2. İrtibat Bilgisi

"e-tuğra Sİ dokümanı" ile ilgili iletişim bilgileri aşağıdadır.
E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
Adres: Ceyhun Atıf Kansu Cad. Gözde Plaza No:130/58 Balgat Ankara
Telefon: 0-312-473 56 90
Faks: 0-312-473 56 91
Çağrı Merkezi: 0-850-532 23 14
Teknik Destek: 0-850-532 23 12
E-posta: info@e-tugra.com.tr , destek@e-tugra.com.tr

Web: http://www.e-tugra.com.tr – http://www.e-tugra.com

İptal Talebi İrtibat Bilgileri

Adres: Ceyhun Atıf Kansu Cad. Gözde Plaza No:130/58-59 Balgat Ankara
Teknik Destek Telefon: 0-850-532 23 12
E-posta: revoke@e-tugra.com.tr , iptal@e-tugra.com.tr
Web: http://www.e-tugra.com.tr – https://helpdesk.e-tugra.com.tr/submit_ticket

1.5.3. "e-tuğra Sİ dokümanı"nın Uygunluğunu Belirleyen Kişi

"e-tuğra Sİ dokümanı"a ve uygunluğunu ve uygulanabilirliğini yetkili "e-tuğra" güvenli personeli ve üst yönetimi denetler.

1.5.4. "Sİ" Onaylama Prosedürü

"e-tuğra" yetkilileri "Sİ" dokümanı ve "e-tuğra" "ESHS" işleyişine yönelik ilkeler ile ilgili denetim çalışmalarını düzenli olarak sürdürürler. Denetim çıktıları doğrultusunda ve/veya işleyiş süreçlerinde değişikliğe gidilmesi durumunda "Sİ" üzerinde değişiklik veya yenileme yapılır. "Sİ" üzerindeki değişiklikler veya yeni sürümler yetkili "e-tuğra" güvenlik forumunun ve üst yönetiminin onayına sunulur.

1.6. Kısaltmalar ve Tanımlar

1.6.1. Kısaltmalar

KISALTMA	AÇIKLAMA/TANIM
"AAA"	Açık Anahtarlı Altyapı (PKI - Public-Key Infrastructure)
"BTK"	Bilgi Teknolojileri ve İletişim Kurumu
"CEN"	Comité Européen de Normalisation - Avrupa Standardizasyon Komitesi
"CRL"	Certificate Revocation List (Bkn "SİL")
"CSR"	Certificate Signing Request – Sertifika İmzalama Talebi
"CWA"	CEN Workshop Agreement- CEN Çalıştay Kararı
"ÇSDP"	Çevrimiçi Sertifika Durum Protokolü (OCSP - Online Certificate Status Protokol)
"DN"	Distinguished Name – Ayırt Edici İsim
"DNS"	Domain Name System – Alan Adı Sistemi
"EAL"	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
"ESHS"	Elektronik Sertifika Hizmet Sağlayıcı
"ETSI TS"	ETSI Technical Specifications - ETSI Teknik Özellikleri
"ETSI"	European Telecommunication Standartization Institute - Avrupa Telekomünikasyon Standartları Enstitüsü
“e-tuğra”	E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
"FKM"	Felaket Kurtarma Merkezi
"IETF RFC"	Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi
"IETF"	Internet Engineering Task Force - İnternet Mühendisliği Görev Grubu
"ISO/IEC"	International Organisation for Standardisation / International Electrotechnical Commitee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
"KB"	Kayıt Birimi
"KIS"	Kod İmzalama Sertifikası
"NES"	Nitelikli Elektronik Sertifika
“NESİ”	Nitelikli Elektronik Sertifika İlkeleri
“NESUE”	Nitelikli Elektronik Sertifika Uygulama Esasları
"OCSP"	Online Certificate Status Protokol (Bkn "ÇSDP")
"OID"	Object Identifier - Nesne betimleyicisi.
"PKI"	Public-Key Infrastructure (Bkn "AAA")
"Sİ"	Sertifika İlkeleri
"SİL"	Sertifika İptal Listesi (CRL - Certificate Revocation List)

"SSL"	Secure Sockets Layer
"SUE"	Sertifika Uygulama Esasları
"TC"	Türkiye Cumhuriyeti
"TCKN"	Türkiye Cumhuriyeti Kimlik Numarası
"TSE"	Türk Standartları Enstitüsü

1.6.2. Tanımlar

KAVRAM	AÇIKLAMA/TANIM
"Açık Anahtar"	"AAA" yapısında, Çift anahtarlı şifreleme algoritmasında üçüncü kişilere de açık olan kriptografik anahtar. ("Kanun"da imza doğrulama verisi olarak isimlendirilmiştir.)
"Açık Anahtar Altyapısı" ("AAA")	Matematiksel bağlantısı bulunan kriptografik anahtar çiftlerine dayalı ve sertifika tabanlı bir kriptografik sistemin kurulması ve işletilmesini sağlayan mimari yapı, teknikler, uygulamalar ve düzenlemeler bütünü.
"Aktivasyon"	"NES" sahipleri için, İmza oluşturma verisi erişim şifresinin, kendisi tarafından belirlenmesine imkân sağlayan interaktif güvenli yöntem.
"Alt Kök Sertifikası"	"ESHS"nin "AAA" hiyerarşisi içerisinde "Güven Merkezi" tarafından oluşturulmuş, "ESHS" kök sertifikasının imzasını taşıyan ve son kullanıcı sertifikalarını imzalama amaçlı kullanılan sertifika.
"Anahtar"	İmza oluşturma veya imza doğrulama verilerinden herbiri.
"Arşiv"	"ESHS"nin saklamakla yükümlü olduğu her türlü bilgi, belge, evrak ve elektronik veri.
"Ayırt Edici İsim Alanı"	Sertifika sahibinin veya sertifikayı ve kuruluşun kimlik bilgilerini içeren, içinde CN, O, OU, T, L, C ve SERIALNUMBER gibi sertifika tipine göre uygun bilgi ve içerikle doldurulan alt alanlara sahip bilgi alanı.
"Başvuru Yöntemleri"	"ESHS" ile Başvuru Sahibi" arasında başvurunun yapılması, sertifika sahibinin kimliğinin tespiti, gerekli evrakların hazırlanması, sertifika ücretlerinin ödenmesi, evrakların saklanması, sertifikaların yayınlanması ve sertifika sahibi'ne iletilmesi, sertifika iptal, yenileme ve askı taleplerinin iletimindeki usuller gibi hususların belirlendiği teknik ve idari süreçlerden oluşan yöntemler. Bu yöntemlere www.e-tugra.com.tr adresinden ulaşılabilir.
"Çevrim İçi Sertifika Durum Protokolü" ("ÇSDP")	Sertifikaların geçerlilik durumunun üçüncü kişilere duyurulması için sertifika durum bilgisinin çevrim içi olarak kesintisiz alınmasını sağlayan standart protokol.
"Dizin"	Geçerli sertifikaları yayınlamak amacıyla içinde bulunduran elektronik depo.

"Elektronik İmza Kanunu	23 Ocak 2004 tarih 25355 sayılı Resmî Gazete'de yayımlanan 5070 Sayılı Kanun.
"Elektronik İmza"	Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri.
"Elektronik Sertifika Hizmet Sağlayıcısı"	Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler.
"Elektronik Veri"	Elektronik, optik veya benzeri yollarla elektronik ortamda üretilen, taşınan veya saklanan kayıtlar.
"Erişim Şifresi"	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola.
"Gizli Anahtar"	Çift anahtarlı şifreleme algoritmasında sadece anahtar sahibinin uktesinde olan kriptografik anahtar. (Kanun'da imza oluşturma verisi olarak isimlendirilmiştir.)
"Güven Merkezi"	"ESHS" yapısında yer alan, Kayıt Birim'lerin den gelen sertifika talepler doğrultusunda başvuru onay ve sertifika üretimi yapan, sertifika iptal işlemlerini gerçekleştirilen, sertifika kayıtları ile sertifika iptal durum kayıtlarını yaratan, işleten ve yayımlayan birim.
"Güvenli e-imza Paketi"	Nitelikli elektronik sertifika ve güvenli elektronik imza oluşturma aracından oluşan "ESHS" tarafından "Sertifika Kullanıcıları"na sağlanan hizmet ve ekipmanlar bütünü. "Güvenli e-imza Paketi"nin fiyatları ile içerdiği ekipmanlar ve hizmetlere ilişkin detaylı açıklamaya www.e-tugra.com.tr web adresinden erişilebilir.
"Güvenli Elektronik İmza Doğrulama Aracı"	Kanunun 7'nci maddesinde sayılan niteliklere sahip: a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren, b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan, d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren, f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan ve CWA 14171 standardına uygun imza doğrulama araçları.
"Güvenli Elektronik İmza Oluşturma Aracı"	Kanunun 6'ncı maddesinde sayılan niteliklere sahip: a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

	b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini, Sağlayan ve ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL4+ seviyesinde olan araçları.
"Güvenli Elektronik İmza"	Güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, e) Kanunun 4'üncü maddesinde sayılan niteliklere sahip, Kanunun hariç tuttuğu işlemler dışında elle atılan imzayla aynı hukuki sonucu doğuran Elektronik imzadır.
"İmza Doğrulama Aracı"	Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı.
"İmza Doğrulama Verisi"	Bknz: "Açık Anahtar"
"İmza Oluşturma Aracı"	Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı.
"İmza Oluşturma Verisi"	Bknz: "Gizli Anahtar"
"İmza Sahibi"	Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan "NES" sahibi gerçek kişi.
"İptal Durum Kaydı"	Geçersiz süresi dolmamış sertifikaların iptal bilgisinin yer aldığı, iptal zamanının tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği kayıt.
"Kanun"	15 Ocak 2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu.
"Kayıt Birimi"	"e-tuğra"ya bağlı olarak faaliyette bulunan, Sertifika Sahipleri ile "Kurumsal Başvuru Sahipleri"nin sertifika başvurularını alan, ilgili kimlik tanımlama ve doğrulama süreçlerini yürüten, sertifika taleplerini onaylayarak "Güven Merkezi"ne yönelten, "ESHS" faaliyetleri kapsamında müşteri ilişkilerini yöneten alt birimlere sahip "e-tuğra"nın yetkili birimleri ve onların personelleri.

"Kimlik Bilgileri"	"Sertifika Kullanıcısı"nın Adı-Soyadı, Türkiye Cumhuriyeti Kimlik Numarası veya Pasaport Numarası, doğum yeri, doğum tarihi ve uyruğu
"Kod İmzalama Sertifikası" ("KIS")	Bilgisayarda çalıştırılabilen bir yazılım kodunun kaynak sahibini doğrulayan sertifika.
"Kök Sertifika"	"ESHS" kurumsal kimlik bilgilerini "ESHS" imza doğrulama verisine bağlayan, "Güven Merkezi" tarafından üretilen ve kendi imzasını taşıyan, "ESHS"nin ürettiği diğer tüm sertifikaların doğrulanabilmesi için "ESHS" tarafından yayımlanan sertifika.
"Kurum"	Bilgi Teknolojileri ve İletişim Kurumu.
"Kurumsal Başvuru Sahibi"	"ESHS" ile Kurumsal Başvuru Sözleşmesi akdetmiş olan ve bu sözleşme hükümleri ve "Yönetmeliğin" 3. ve 9. maddeleri uyarınca çalışanları veya müşterileri veya üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusunda bulunan tüzel kişilik.
"Kurumsal Başvuru Yetkilisi"	"Sertifika Kullanıcısı" adına "NES" düzenlenmesi için "ESHS"ye bildirilecek olan bilgileri "Yönetmeliğin" Mad. 9/1.de belirtilen belgelere dayanarak tespit eden ve "Kurumsal Başvuru Sözleşmesi" içerisinde kendisiyle ilgili belirtilen işlemleri "Kurumsal Başvuru Sahibi" adı ve hesabına yerine getiren "Kurumsal Başvuru Sahibi"nin çalışanı.
"Kurumsal Başvuru"	Bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusu.
"Mali Sorumluluk Sigortası"	"ESHS"nin, "Kanun"dan veya uygulamalardan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigorta.
"Nitelikli Elektronik Sertifika" ("NES")	5070 Sayılı Kanun'un 9. Maddesinde içerik olarak; "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"in 5. Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
"Özetleme Algoritması"	İmzalanacak elektronik verilerin sabit uzunlukta bir özetinin çıkarılmasında kullanılan algoritma.
"Özne"	Sertifikanın CN alanında yer alan kişi veya sunucu adı.
"Secure Sockets Layer" ("SSL")	İnternet haberleşmesinde veri gizliliğinin sağlanması, veriyi sunan sunucu kaynağının doğrulanması ve/veya veriyi alan istemcinin doğrulanması amacıyla geliştirilmiş güvenlik protokolü.
"Sertifika İlkeleri"	Sertifikaların belli bir topluluk ve/veya genel güvenlik gereklilikleri olan uygulamalar bakımından kabul edilebilirliğini belirten kurallar bütününe ve ESHS'nin işleyişi ile ilgili genel kuralları içeren belgeye "Sertifika İlkeleri" denir. "Sertifika İlkeleri", Elektronik Sertifika Hizmet Sağlayıcıları tarafından umuma açıklanan yönelik bir belgedir. "ESHS" tarafından yayınlanan "Sİ"ye, "Sertifika Kullanıcı"ları uymak zorundadır. "Sİ"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, güncel ve önceki sürümlerine "ESHS"nin web sitesinden erişilebilir.

"Sertifika İmzalama Talebi" ("CSR")	Talep sahibi tarafından üretilen ve sahip olduğu gizli anahtarla imzaladığı sertifika talebi.
"Sertifika İptal Listesi"	İptal edilmiş sertifikaların üçüncü kişilere duyurulması amacıyla "ESHS" tarafından yayımlanan elektronik dosya.
"Sertifika Kullanıcısı" - "Sertifika Sahibi"	Adına "ESHS" tarafından sertifika düzenlenen gerçek veya tüzel kişilik. Bu doküman içerisinde geçen "Sertifika Sahibi" kavram "Sertifika Kullanıcısı" ile eş anlamlı olarak kullanılmaktadır.
"Sertifika Uygulama Esasları"	"Sertifika Sahipleri" başta olmak üzere "Sİ" içerisinde tanımlanan her bir tarafın "Sİ" içinde tanımlı operasyonları gerçekleştirmek için uymak zorunda olduğu gerekliliklerin tespit edildiği, uygulamaların ve prosedürlerin açıklandığı, belli süreçler içerisinde güncellenen ve "ESHS" tarafından umuma yapılan bir açıklamadır. "SUE"ye, duruma göre zaman zaman yapılabilecek değişiklikler de dahil olmak üzere, "ESHS"nin web sitesinden erişilebilir.
"Tebliğ"	6 Ocak 2005 tarih 25692 sayılı Resmî Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ".
"Yönetmelik"	6 Ocak 2005 tarih 25692 sayılı Resmî Gazete'de Bilgi Teknolojileri ve İletişim Kurumu tarafından yayımlanan "Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik".
"Zaman Damgası İlkeleri"	Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren doküman.
"Zaman Damgası Uygulama Esasları"	Zaman damgası ilkelerinde yer alan ilkelerin nasıl uygulanacağını anlatan döküman.
"Zaman Damgası"	Elektronik verinin, üzerinde yapılan işlemin zamanın tespit edilmesi amacıyla, "ESHS" tarafından elektronik imzayla doğrulanan kayıt.

2. YAYIN VE BİLGİ DEPOSU SORUMLULUKLARI

"e-tuğra", Elektronik Sertifika Hizmet Sağlayıcılığı kapsamında sertifika hizmetleriyle ilgili tüm gerekli doküman ve kayıtları hazırlamak ve saklamakla sorumludur, sertifika hizmetlerinin etkin bir şekilde yürütülmesi ve sertifika kullanımının güvenilirliğinin ve sürekliliğinin sağlanması için bazı doküman ve bilgileri erişime açık bulundurur.

2.1. Bilgi Deposu

"e-tuğra" oluşturduğu Kök ve Alt Kök Sertifikaları, "SİL"leri, "SUE" ve "Sİ" dokümanlarını, "ESHS" işleyişi içerisinde kullandığı sözleşmeleri, bilgilendirici dokümanları ve ilgili görsel ve işitsel yayımları bilgi deposunda yayınlar. Bilgi deposu sertifika sahiplerinin, üçüncü kişilerin ve ilgili herkesin erişimine 7/24 hizmet verecek şekilde erişime açık bulundurulur. Bilgi Deposu hizmeti 24 saatten fazla erişme kapalı olamaz.

"e-tuğra" ilgili doküman ve kayıtları yayımlamak için üçüncü bir kişi ya da kuruluş kullanmaz.

2.2. Sertifika Bilgilerinin Yayımlanması

"e-tuğra" bilgi deposunda sertifika hizmetlerinin yürütülmesine ilişkin bilgiler herkesin erişimine açık tutulur. "ESHS" iç işleyişine ait özel kurumsal prosedür ve talimatlar ile ticari gizli bilgiler bu kapsamın dışındadır. "e-tuğra" bilgi deposuna yayınlanan temel bilgiler şunlardır.

- "e-tuğra" Kök ve Alt Kök Sertifikaları
- "e-tuğra" Zaman Damgası ve "ÇSDP" Sertifikaları
- "e-tuğra" tarafından üretilen sertifikalar ve sertifika sahibinin yayınlanması için yazılı rızası olan Sertifikalar
- "e-tuğra" Güncel "SİL" dosyaları
- "Sİ" ve "SUE" dökümanları
- "e-tuğra" Sertifika Başvuru ve Kullanıcı Sözleşmeleri,
- Kurumsal Başvuru Sözleşmeleri,
- Sertifika başvurularına ilişkin dokümanlar
- Bilgilendirme dokümanları ve ilgili görsel ve işitsel yayımlar

Bu bölümde sözü geçen bilgilere erişim, "e-tuğra"ya ait http://www.e-tugra.com.tr web sitesinden kamuya açık olarak sağlanır.

2.3. Yayımın Zamanı ve Sıklığı

- "SUE" ve "Sİ"de yapılan güncellemeler ve yeni sürümler, eski sürümlerle birlikte bilgi deposunda yayımlanır.
- "e-tuğra" Kök ve Alt Kök Sertifikaları ve yayınlanması izin verilen sertifikalar düzenlendikleri tarihte yayınlanır.
- Sertifika Durum Bilgileri "Sİ" 4.9.7.' ve "Sİ" 4.9.10.'a göre yayınlanır.
- NES için SİL'ler, 6 (altı) saatte bir olmak üzere günde 4 (dört) kez ve 24 (yirmi dört) saatlik geçerlilik süresiyle yayımlanır.

2.4 Bilgi Deposu Erişim Kontrolleri

Bilgi deposu 7/24 hizmet verecek şekilde tüm ilgililerin erişimine açık tutulur. Bilgi deposundaki bilgilerin geçerliliği ve doğruluğu konusunda yetkili "e-tuğra" personeli düzenli kontroller yapar ve her türlü güvenlik önlemini alır.

3. TANIMLAMA VE KİMLİK DOĞRULAMA

“e-tuğra”, yeni sertifika başvurusunda bulunan, mevcut sertifikasını yenilemek isteyen kişilerin kimlikleri veya adına sertifika talebinde bulunulan web, elektronik posta ve benzeri sunucuların elektronik adres bilgileri ile sertifika içerisinde yer alacak bilgileri, yasal ve teknik gerekliliklere göre gerekli görülen tüm belgelere ve resmi kaynaklara dayandırarak doğrular.

3.1. İsimlendirme (İlk Kayıt)

3.1.1. İsim Tipleri

Sertifikalarda sadece ITU X.500 biçiminin desteklediği isim tipleri kullanılır.

3.1.2. İsimlerin Anlamlı Olması Gerekliliği

Üretilen sertifikalardaki isimler belirsizlikten uzak ve anlamlıdır.

3.1.3. Sertifika Sahiplerinin Anonimliği, Takma İsim Kullanımı, Sertifika Sahiplerinin İsimlerinin Gizlenmesi

“e-tuğra”, ürettiği sertifikalarda anonim veya takma isim kullanmaz.

3.1.4. Değişik İsim Tiplerini Yorumlamak İçin Kurallar

Üretilen sertifikalarda yer alan isimler X.500 ayırt edici isim biçimine uygun olarak yorumlanır ve hazırlanır.

3.1.5. İsimlerin Benzersizliği

“e-tuğra”, oluşturduğu sertifikalarda, ayırt edici isim alanında yer alan bilgilerle sertifika sahiplerinin eşsiz biçimde belirlenmesine olanak sağlar. Mevzuata bağlı nedenlerle sertifika tiplerine göre ayırt edici isim alanları farklı bilgileri içerir. “e-tuğra”nın oluşturduğu “NES”ler de, farklı kişilere ait “NES”ler deki kimlik bilgilerinin benzersiz olması sağlanır.

3.1.6. Ticari Markaların Tanınması, Doğrulanması ve Rolü

Sertifika sahipleri, sertifika başvurularında ticari marka isimlerinin doğru biçimde yer almasından ve kullanılmasından sorumludur. Başvuru sahiplerinin, tüm sertifika başvurularında başkalarının fikri mülkiyet haklarını ihlal eden isimler kullanması yasaktır. “e-tuğra”, sertifika başvurusunda ticari marka isimlerinin kullanımına ilişkin bir ihlali tespit ederse başvuruyu reddetme, sertifikayı askıya alma veya sertifikayı iptal etme hakkını saklı tutar.

3.2. İlk Kimlik Doğrulaması

3.2.1. İmza Oluşturma Verisinin (Gizli Anahtarın) Zilyetliğinin Kanıtlanması Metodu

“NES” imza oluşturma ve doğrulama verileri sadece “e-tuğra” tarafından oluşturulmaktadır. “NES”in ve güvenli elektronik imza oluşturma aracının “NES” sahibine imza karşılığı teslim edilmesi halinde, “NES” sahibinin imza oluşturma verisine sahip olduğu kabul edilir.

3.2.2. Tüzel Kişiliğin ve Alan Adının Doğrulanması

Bir sertifikada bir tüzel kişiliğin isminin veya unvanının yer alması halinde, sertifika türüne göre aşağıdaki doğrulama yöntemleri uygulanır. Tüzel kişiliğin doğrulanmasına ilişkin süreç burada belirlenen şartlara bağlı kalmak kaydıyla "e-tuğra" prosedürlerinde belirtilen şekilde yürütülür.

Kurumsal başvurularda ve/veya "NES" içerisine ilgili tüzel kişi adına yetki ile ilgili bilgi konulması gerektiği takdirde, tüzel kişinin kimliği resmî belgelere dayanılarak doğrulanır.

3.2.3. Gerçek Kişilerin Kimliğinin Doğrulanması

"NES" başvurularında gerçek kişinin kimliği, yasal düzenlemelerle belirlenen, nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli bir resmi belgeye dayanılarak tespit edilir. Kimliğin dayandırıldığı resmi belgelerin aslı "e-tuğra" veya Yetkili Kayıt Birimleri tarafından görülür, fotokopisi alınarak teyit edilir.

İkinci ve daha sonraki başvurularda, geçerliliği devam eden son sertifikanın kullanım süresi sonundan itibaren 6 (altı) ay geçmiş olması veya içeriğinde "DN" alanındaki bilgide veya adında değişiklik olması halinde tekrar yüz yüze kimlik tespiti yapılır.

Daha sonraki başvurularda kimlik tespitine ihtiyaç olmaması durumunda, Kimlik tespiti, telefon, faks veya e-posta gibi yollarla "e-tuğra" prosedürlerine ve talimatlarına göre gerçekleştirilir.

"NES" içeriğinde mesleki unvanın da yer almasının istendiği durumlarda, mevzuata göre düzenlenmiş resmi belgelerin ibrazı gerekmektedir.

3.2.4. Doğrulanmayan Başvuru Bilgileri

"NES" sahibinin "NES" içerisinde yer alan bilgileri dışındaki bilgilerin "e-tuğra" tarafından doğrulanmasına gerek yoktur. "NES" başvurularında e-posta adresi sertifika başvuru sahibinin yazılı beyanıyla sertifika içeriğinde yer alır.

Sertifikalarda bulunabilen "L", "S" ve "OU" gibi ayırt edici isim alanında yer alan diğer bilgilerde de sertifika başvuru sahibinin beyanına göre doğru kabul edilir ve sertifika içeriğinde yer alır.

3.2.5. Yetkinin Doğrulanması / Kanıtlanması

"NES" içerisine ilgili tüzel kişi adına yetki ile ilgili bilgi konulması gerektiği takdirde, tüzel kişinin kimliği ve "NES" sahibinin yetkileriyle ilgili bilgiler resmî belgelere dayanılarak doğrulanır.

"Kurumsal Başvuru Sahibi" tarafından yapılan "NES" başvurularında "Kurumsal Başvuru Yetkilisi" için yetki doğrulaması yapılır.

3.2.6. Karşılıklı Çalışabilirlik Kriterleri

"e-tuğra" bir diğer Sertifika Sağlayıcı ile beraber çalışabilirlik amacıyla sertifikasyon işlemi yapmaz.

3.3. Anahtarlama Yenileme için Tanımlama ve Kimlik Doğrulama

3.3.1. Rutin Yeniden Anahtarlama için Tanımlama ve Kimlik Doğrulama

"NES" ler geçerlilik süresi içerisinde yenilenebilir, geçerlilik süresi sona ermiş "NES"ler için yeniden anahtarlama yapılamaz. Yenileme talepleri "e-tuğra" web portali üzerinden online başvuru yaparak,

“e-tuğra” genel merkez adresine ulaşarak veya Kayıt Birimleri aracılığı ile yapılabilir. Anahtar yenileme işlemlerinde yüzyüze kimlik tespiti yapma şartı aranmaz.

Şüpheli durumlarda “e-tuğra” yeniden kimlik tespiti talebinde bulunabilir. Geçerlilik süresi sona ermeyen “NES”lerde anahtar yenileme işlemleri sırasında, “NES” sahibi tarafından talep edilen “NES” içerisindeki herhangi bir bilgi değişiklik için bu değişikliğin resmi belgelere dayandırılması gerekir ve anahtar yenileme işlemi yapılamaz, yeni bir başvuru süreci gerektirir ve kimlik tespiti yapılması gerekir.

Sertifika sahibinin başvurusu ile yenileme başvurusu arasında geçen sürede “e-tuğra” sertifika hizmetlerinin sağlanmasına ilişkin kayıt ve şartlarda değişiklik oluşmuş ise bu değişiklikler web sitesinden yayınlanarak sertifika sahiplerine duyurulur.

3.3.2. Sertifika İptali Sonrası Yeniden Anahtarlama İçin Tanımlama ve Kimlik Doğrulama

Sertifika iptalinden sonra yeniden anahtarlama yapılmaz, yeniden anahtarlama talebi yeni bir sertifika başvurusu olarak kabul edilir ve sertifika başvurusu ile ilgili tüm prosedürler uygulanır.

3.4. İptal Talebi İçin Tanımlama ve Kimlik Doğrulama

“NES”ler, “NES” sahipleri, “NES” sahibi tarafından izin verilmesi halinde kurumsal başvuru sahipleri ve üçüncü kişiler tarafından iptal edilebilir. İşbu “Sİ” VE İLGİLİ “SUE”de belirtilen şartların gerçekleşmesi halinde “e-tuğra” da “NES”i kendi inisiyatifi ile iptal edilebilir. Kurumsal bilgi içeren “NES”lerde kurumu temsile yetkili kişiler tarafından da iptal edilebilir.

Başvuru sahibi ilk başvuruyu yapan gerçek kişi değilse, başvuru sahibinin tüzel kişi adına hareket etme yetkisine sahip olduğunu destekleyecek resmi bir belge istenir.

4. SERTİFİKA YAŞAM ZİNCİRİ OPERASYONEL GEREKLİLİKLER

"e-tuğra", sertifikalarını işbu "Sİ" dokümanında yer alan ilkelere göre üretilir ve yaşam döngüsünü yönetir.

4.1. Sertifika Başvurusu

4.1.1. Kim "Sertifika" Başvurusunda Bulunabilir

"e-tuğra" tarafından belirlenen prosedürleri yerine getiren, yasal bir engeli olmayan tüm gerçek kişiler "NES" başvurusunda bulunabilir.

Çalışanları, müşterileri, üyeleri veya hissedarları "Kurumsal Başvuru"da bulunacak olan tüzel kişiler "NES" başvurusunda bulunabilirler.

4.1.2. "Sertifika" Başvuru, Kayıt Süreci ve Sorumluluklar

Sertifika başvurusu, kayıt ve anahtar üretimi olmak üzere iki adımdan oluşur: Kayıt, sertifika başvurusunun dayanak belgelerine göre doğrulanması ve eksiksiz ve doğru biçimde kaydedilmesidir. Anahtar üretimi ise, açık ve gizli anahtar çiftinin sertifika başvuru sahibi veya "e-tuğra" tarafından üretilmesidir. Anahtar çiftinin sertifika başvuru sahibi tarafından üretilmesi durumunda, açık anahtarın belirlenen prosedür ve standartlara göre "e-tuğra"ya elektronik ortamda gönderilmesi gerekir.

"NES" Başvurusu:

"NES" başvuruları çeşitli Başvuru Yöntemleri ile yapılabilmektedir. "NES" başvuru sahibi, sertifika başvurusunda bulunmak için, şahsen "e-tuğra"ya veya "e-tuğra" web sitesinde yayınlanan yetkili "KB"ye giderek veya "e-tuğra" web sitesinde yer alan Başvuru Formu"nu doldurarak "NES" başvurusunda bulunabilir.

Gizli ve açık anahtarlar "NES"lerin kartlara basılması sırasında "e-tuğra" tarafından kart üzerinde üretilir.

Kurumsal "NES" Başvurusu:

"Kurumsal Başvuru", bir tüzel kişiliğin çalışanları veya müşterileri veya üyeleri veya hissedarları adına "NES" başvurusunda bulunmasıdır. "Kurumsal Başvuru"larda, "Kurumsal Başvuru Sahibi", "e-tuğra" ile akdetmiş olduğu "Kurumsal Başvuru Sözleşmesi Hükümleri" uyarınca kendi üstlendiği yükümlülükleri kendi adı ve hesabına yerine getirmek üzere "Kurumsal Başvuru Sahibi" ile arasında geçerli bir hizmet akdi bulunan bir personelini "Kurumsal Başvuru Yetkilisi" olarak atar. "e-tuğra"ya kurumsal başvuru , tüzel kişilik ile "e-tuğra" arasında hazırlanan "Kurumsal Başvuru Sözleşmesi"nde belirtilen usullerde yapılır.

4.2. Sertifika Başvuru Süreci

4.2.1. Kimlik Tanılama ve Doğrulama İşlemlerinin Gerçekleştirilmesi

"Kayıt Birimi" yetkilileri "NES" başvuru sahiplerinin, kurumsal başvuru sahiplerinin ve kurumsal başvuru yetkililerinin Bölüm 3.2 ve Bölüm 4.1'de belirtilen ilkelere göre kimlik doğrulamalarını yaparlar.

"NES" başvurusu sırasında, başvuru sahibinin kimliği yasal düzenlemeler uyarınca resmi belgelere dayandırılarak doğrulanır.

4.2.2. "Sertifika" Başvurularının Kabulü ve Reddi

"e-tuğra" kendisine yapılan başvuruları kabul etmekte veya reddetmekte serbesttir. Sertifika başvurusu kabul edilebilmesi için aşağıdaki koşulların tamamlanması gerekmektedir:

- Bölüm 4.1.2. de yer alan başvuru yöntemlerinin herhangi birinin tamamlanmış olması,
- Bölüm 3.2'de açıklanan ilkeler ve "e-tuğra" başvuru prosedürlerine göre gerekli form ve belgelerin eksiksiz olarak tamamlanmış olması,
- Sertifika bedelinin ödenmiş olması ile sertifika başvuruları kabul edilir.

Yukarıdaki koşullar sağlanmış olsa bile aşağıdaki durumlar oluştuğunda başvuru reddedilebilir ve başvuru sahibi bilgilendirilir.

- Bilgi ve belgelerin doğrulanmasına ilişkin sorgulamalara başvuru sahibinin zamanında veya tatminkâr yanıt vermemesi.
- Başvuruda sertifika üretilmesinin, "e-tuğra"nın itibarının zarar görebileceğine ilişkin kuvvetli bir kanaatinin oluşması.

"e-tuğra" herhangi başvuru reddedildiğinde geçerli bir sebep göstermek zorunda değildir.

4.2.3. "Sertifika" Başvuruları İşleme Süreci

"E-tuğra"ya ulaşan "NES" başvurularının alınmasının ardından sertifika başvurularının işlenme süreci en fazla 5 (beş) iş günüdür. Başvuruların kabulünden sonra üretim süreci en fazla 1 (bir) iş günüdür. "NES" üretimleri smartcard stok durumuna göre üretimi mecburi durumlarda 45 takvim günü olabilir.

Sertifika başvurularının işlenmesine ilişkin süreler, sertifika başvurularının Bölüm 3.2'de yer alan ilkeler ve "e-tuğra" prosedürlerine göre eksiksiz ve doğru olması halinde geçerlidir.

4.3. Sertifika Üretimi

4.3.1. Sertifika Üretimi Sırasındaki "ESHS" Faaliyetleri

Bölüm 4.2.2 de belirtilen ilkelere göre kabul edilen sertifika başvuruları "e-tuğra" "Güven Merkezi"nde başvuruların kabulünden sonra işlenerek üretilir.

Bölüm 4.2'de belirtilen başvuru süreçlerinin tamamlanarak başvurunun kabul edilmesinden sonra "e-tuğra" "güvenli personel"i tarafından "Güven Merkezi" içerisinde iki kademeli onay sürecinden geçtikten sonra üretilir.

4.3.2. Sertifika Üretimiyle İlgili Sertifika Sahibinin Bilgilendirilmesi

Sertifikanın üretimi gerçekleştikten sonra sertifika sahibine SMS veya e-posta aracılığı ile sertifikanın üretildiğine dair bilgilendirme mesajı gönderilir.

4.4. Sertifikanın Kabulü

4.4.1. Kabulün Şekli

"e-tuğra" tarafından oluşturulan sertifikayı, sertifika sahibinin teslim alması sertifikanın kabulü sayılır. Tüm sertifika tipleri için, sertifika sahipleri, sertifikayı yüklemeden veya kullanmadan önce sertifika içeriğindeki bilgileri gözden geçirmek ve doğrulamakla, doğru olmayan, eksik, hatalı veya başvuruyla tutarsız bilgiler olması durumunda "e- Tuğra" yı bilgilendirmek ve sertifikanın iptalini talep etmekle

yükümlüdür. Söz konusu bilgi tutarsızlığı "e-tuğra" kaynaklı ise, "e-tuğra" sertifika sahibinin dolduracağı yeni formlar ile sertifika üretimini tekrar yapar.

4.4.2. "ESHS" Tarafından Sertifikanın Yayımlanması

Ancak sertifika sahibinin yazılı izni ile "e-tuğra" tarafından halka açık bir dizinde veya web üzerinden yayımlanır.

4.4.3. Diğer Katılımcıların Sertifika Üretimiyle İlgili Bilgilendirilmesi

İlgili değildir.

4.5. Anahtar Çifti ve Sertifika Kullanımı

4.5.1. Sertifika Sahibi İmza Oluşturma Verisi ve Sertifika Kullanımı

Sertifika sahipleri sertifikasını ve sertifika gizli anahtarını, "SUE", "Sİ", ilgili Kanun, Yönetmelik, Tebliğ ve imzalamış oldukları sertifika kullanıcı sözleşmeleri ile belirlenen yükümlükleri doğrultusunda kullanmak zorundadır. Ayrıca sertifikalar eğer bulunuyorsa kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanılmalıdır.

Sertifika sahibi imza oluşturma verisinin ve erişim verisinin güvenliğini sağlamak ve izinsiz kullanımlarını engellemekle yükümlüdür. Sertifika sahibinin, imza oluşturma verisinin gizliliği veya güvenliği konusunda şüphe duyması, imza oluşturma verisinin, imza oluşturma aracının veya erişim verisinin kaybolması, çalınması veya güvenilirliğinden şüphe duyması halinde derhal "e-tuğra"yi bilgilendirmesi gereklidir.

4.5.2. Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

"e-tuğra" sertifikalarına güvenerek iş ve işlem yapacak olan üçüncü kişiler öncelikle sertifikanın kontrolünü yapmalıdırlar. Sertifika Sahipleri sertifikalarını Kanun, Yönetmelik, Tebliğ ve diğer düzenlemeler ile "Sİ" ve "SUE" kitapçıklarında belirlenmiş kullanım amaçları dâhilinde kullanmakla yükümlüdürler.

Sertifikanın geçerliliğinin kontrolünün makul ve güvenli koşullar altında yapılması durumunda bir tereddüt olması halinde, üçüncü kişiler gerekli tedbirleri alır. Üçüncü kişiler sertifikaya güvenmek için;

- Sertifikanın kullanım amacına uygun kullanıldığını;
- Herhangi bir yanlış işlemin yaralanma, ölüm, çevresel zarara sebep olduğu nükleer tesis, hava trafik kontrol, uçak navigasyon, silah kontrol gibi sistemlerde kullanılmadığını,
- Sertifika içeriğinde yer alan anahtar kullanım durumuyla uyumlu olduğunu,
- Sertifikanın "e-tuğra" tarafından oluşturulduğunu,
- Sertifikanın kendisinin ve dayandığı kök ve alt kök sertifikalarının geçerli olduğunu, kontrol etmekle yükümlüdür. Bu amaçla "e-tuğra" "SİL" ve "ÇSDP" servis hizmetlerini kesintisiz olarak sağlar.

Bu işlemler sırasında, mevzuat ve standartlarca belirlenmiş güvenli yazılım ve donanım araçlarının kullanılması üçüncü kişilerin sorumluluğundadır.

Sertifikaların kontrolünün ve doğrulama prosedürlerinin başarısız olması durumunda sertifikaya dayanarak işlem yapmamalıdır.

"e-tuğra", üçüncü kişilerin imza doğrulama verisi ve sertifika kullanımında söz konusu şartları yerine getirmemelerinden sorumlu değildir.

4.6. Sertifika Yenileme

"e-tuğra" sertifika yenileme işlemleri "NES" için aşağıda açıklanan yenileme süreçlerine tabidir. Sertifika yenileme, sertifika içeriğindeki açık anahtar değişmemek koşulu ile, sertifika geçerlilik süresinin uzatılmasıdır. Sertifika yenilemenin yapılabilmesi için, sertifikanın gizli anahtarının açığa çıkmamış olması zorunludur. Geçerlilik süresi dolan sertifikalar için yenileme başvurusu yapılamaz. Anahtarların güvenliği için, aynı verilere sahip bir sertifikanın toplam geçerlilik süresi 3 (üç) yıldan fazla olamaz.

4.6.1. Sertifika Yenilemeyi Gerektiren Durumlar

Sertifikalar ancak sertifikaların geçerlilik sürelerinin sona ermesinden önce ve sertifika içeriğinde değişiklik gerektirecek bir durumun bulunmaması halinde, sertifika sahibinin talebi üzerine yenilenebilir. Sertifika geçerlilik süresi içinde yenileme başvurusunun yapılmış ve kabul edilmiş olması koşuluyla, süresi dolmuş sertifika da yenilenebilir.

4.6.2. Yenileme Talebinde Bulunabilecek Kişiler

Sertifika sahibi veya sertifika sahibini temsile yetkili kişi tarafından yenileme talebinde bulunulabilir.

4.6.3. Sertifika Yenileme Talebinin İşlenmesi

Yenileme talepleri "e-tuğra" web sitesinden veya "KB"ler aracılığıyla yapılabilir. Yenileme talebinin web sitesi üzerinden yapılması halinde, sertifika yenilenmesine ilişkin başvuru formu doldurulur ve form yenileme talebinde bulunan sertifika sahibinin güvenli elektronik imzası ile imzalanır. "e-tuğra" yenileme talebinde bulunan sertifika sahibinin güvenli elektronik imzasını doğrulayarak "NES" sahibinin kimlik doğrulamasını yapar. "KB"ye yapılan yenileme başvurularında "KB" yetkilisi sertifika sahibinin nüfus cüzdanı, pasaport, sürücü belgesi gibi resmi kimlik belgelerine dayanarak kimlik doğrulaması yapar. Kimlik doğrulaması aşamasının tamamlanmasından ve gerekli onaylama prosedürlerinin ve ödeme kontrollerinin gerçekleştirilmesinden sonra yeni sertifika oluşturulur.

4.6.4. Yenilenmiş Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2'de yer alan ilkeler uygulanır.

4.6.5. Yenilenen Sertifikanın Kabulü

"NES" yenileme prosedürlerinde son adım olan sertifika sahibinin yeni sertifikasını yüklemesi sertifika yenilenmesinin kabulü sayılır. Bölüm 4.4.1'de yer alan ilkeler uygulanır.

4.6.6. "ESHS" Tarafından Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2'de yer alan esaslar uygulanır.

4.6.7. Diğer Katılımcıların Yeni Sertifika Üretimiyle İlgili Bilgilendirilmesi

İlgili değildir.

4.7. Sertifikaların Yeniden Anahtarlanması

“e-tuğra” aşağıda belirtilen özel durumlarda yeniden anahtarlama yapılır. Bu durum dışında yeniden anahtarlama yapılmaz. Yenileme işlemleri sertifika yenileme ile yapılmaktadır. Yeniden anahtarlama yapılması gereken durumlarda “NES” iptal edilir ve “NES” başvurusu süreçleri işletilerek yeni bir “NES” oluşturulur.

4.7.1. Anahtar Yenilemeyi Gerektiren Durumlar

“NES” için geçerlilik süresinin ilk 1 (bir) ayı içinde sertifika sahibinin kartından sertifikanın silinmiş olması, kartın kaybolması veya kartın bir biçimde çalışamaz olması durumunda, ilk başvuruda sağlamış olduğu hiçbir bilginin değişmemiş olması ön koşulu ile yeniden belge istenmeksizin, bir defaya mahsus olmak üzere anahtar yenilemeyle yeni bir sertifika üretilir.

4.7.2. Anahtar Yenileme Talebinde Bulunabilecek Kişiler

“NES” için sertifika sahibi gerçek kişidir.

4.7.3. Anahtar Yenileme Talebinin İşlenmesi

Bölüm 4.7.1 ‘de belirtilen koşullara dair bir şüphe olması durumunda, ilgili bilgi ve destekleyici belgeler ve deliller yeniden alınır.

4.7.4. Yeni Sertifikayla İlgili Sertifika Sahibine Bildirim Yapılması

Bölüm 4.3.2’de yer alan ilkeler uygulanır.

4.7.5. Anahtarı Yenilenen Sertifikanın Kabulü

Bölüm 4.4.1’de yer alan ilkeler uygulanır.

4.7.6. "ESHS" Tarafından Anahtarı Yenilenen Sertifikanın Yayımlanması

Bölüm 4.4.2’de yer alan ilkeler uygulanır.

4.7.7. Diğer İlgililere Sertifika üretilmesine İlişkin "ESHS" Tarafından Yapılan Bildirim

İlgili değildir.

4.8. Sertifika Değişikliği

4.8.1. Sertifikalarda Değişiklik Yapılmasını Gerektiren Durumlar

Sertifika içeriğinin değiştirilmesi ancak sertifikanın iptal edilmesi veya sertifika içeriğindeki bir değişiklik gerekmesi durumunda, yeni bir sertifikanın oluşturulması ile gerçekleşebilir. Bu tür bir değişiklik yeni bir sertifika başvuru sürecinin başlatılmasını gerektirir.

4.8.2. Kimler Sertifika Değişiklik Yapılmasını Talep Edebilir

Bölüm 4.1.1’deki ilkeler uygulanır.

4.8.3. Sertifika Üzerinde Değişiklik Yapılmasına İlişkin Taleplerin Süreci

Bölüm 3.2'deki ilkeler uygulanır.

4.8.4. Yeni Sertifika Oluşturulmasına İlişkin Sertifika Başvurusunda Bulunanlara Yapılan Bildirim

Bölüm 4.3.2'deki ilkeler uygulanır.

4.8.5. Değiştirilmiş Sertifikaların Kabulü Sayılan İşlemler

Bölüm 4.4.1'deki ilkeler uygulanır.

4.8.6. "ESHS" Tarafından Sertifika Değişikliklerine İlişkin Yayın

Bölüm 4.4.2'deki ilkeler uygulanır.

4.8.7. "ESHS" Tarafından Diğer Kuruluşlara Sertifika Oluşturulmasına İlişkin Bildirim

İlgili değildir.

4.9. Sertifika İptali ve Askıya Alma

4.9.1. Sertifika İptalini Gerektiren Durumlar

Aşağıda yer alan koşullar sertifikanın iptalini gerektirir:

- Sertifikanın kullanım süresi içinde içerdiği bilgilerin geçerliliğini kaybetmesi durumunda,
- Sertifika sahibinin veya temsile yetkili kişinin talebi, sertifika sahibi, sertifika iptal talebini, "e-tuğra"nın resmi web sitesi üzerinden, çağrı merkezi yoluyla, güvenli elektronik imzalı olarak göndereceği e-posta yoluyla veya yazılı olarak talepte bulunması durumunda,
- Sertifika başvurusunda veya sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması; "e-tuğra" bu şartın oluştuğuna dair makul kanıta dayalı kanaat oluşturabileceği gibi aynı şart sertifika sahibi veya temsili yetkili kişinin bildirimiyle de oluşabilir.
- Sertifika içeriğinde yer alan bilgi veya sertifika sahibi bilgilerinde bir değişiklik olması,
- Sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin veya ölümünün öğrenilmesi,
- Sertifikanın, gizli anahtarın kaybedilmesi, çalınması, ortaya çıkma şüphesinin veya üçüncü kişilerin erişimi ve kullanımı tehlikesinin oluşması,
- Sertifikanın gizli anahtarına erişim şifresinin ortaya çıkması veya benzer bir nedenle sertifika sahibinin gizli anahtar üzerindeki kontrolünü kaybetmesi,
- Sertifikanın gizli anahtarının içinde bulunduğu yazılım veya donanım aracının kaybolması, bozulması veya güvenilirliğini kaybetmesi,
- "e-tuğra"nın, sertifikanın "Sİ" ve "SUE" rehber kitapçıkları ile sertifika taahhütnamesi veya anlaşması hükümlerine aykırı olarak kullanıldığına ilişkin bir bildirim alması veya böyle olduğunun anlaşılması,
- "e-tuğra"nın tamamen kendi takdiri sonucu, sertifikanın verilişi sırasında işbu "Sİ" ve ilgili "SUE" ilişkin bir uygunsuzluk tespit etmesi,

- Sertifikalarının üretiminde kullanılan anahtar uzunluğunun veya kriptografik algoritmaların uygunluğunun ortadan kalkması durumunda,
- Sertifikanın amacı dışında kullanıldığına dair bir kanıtın elde edilmesi halinde,
- "sertifika üretimi sonrası ilgili kayıt birimi aracılığıyla teslim edilecek olan e-imza paketinin 1 (bir) ay içinde sertifika başvuru sahibi tarafından teslim alınmaması veya kurye ile gönderilen e-imza paketinin 1 (bir) ay boyunca sertifika başvuru sahibi tarafından teslim alınmaması,
- Kanun'a dayalı sertifika verme hakkının ortadan kalkması,
- "Kurumsal Başvuru Sahibi" ile "Sertifika Sahibi" arasında "Kurumsal Başvuru"da bulunmaya esas teşkil eden hukuki ilişkinin sona ermesi,
- Sertifika Sahibinin sertifikayı kullanarak icra ettiği kasti bir fiili neticesinde "e- tuğra"nın veya "Kurumsal Başvuru Sahibi"nin zarara uğraması,
- Sertifika Sahibi tarafından hukuka veya "NES" içerisinde yer alan kullanım veya maddi kapsama aykırı amaçlarla kullanıldığının "e-tuğra" veya "Kurumsal Başvuru Sahibi" tarafından tespiti,
- "e-tuğra" kök veya alt kök sertifikalarına ait gizli anahtarların çıkma şüphesinin oluşması veya açığa çıkması,

"e-tuğra"nın sertifika hizmetleri vermeyi durdurması. Alt kök sertifikanın kullanım süresi içinde geçerliliğini kaybetmesi durumunda en geç 7 (yedi) gün içinde iptal edilir.

4.9.2. Kimler İptal Başvurusunda Bulunabilir

Sertifikalar için aşağıda belirtilen kişiler tarafından iptal talebinde bulunabilir;

- Sertifika sahibi,
- Sertifika içerisinde kurum bilgilerinin bulunması halinde kurumun yetkili kişileri, yetkisi bulunması halinde kurumsal başvuru sahipleri,
- Yetkileri doğrultusunda kamu kurumları ve yargı makamları,
- Gerekli durumlarda "e-tuğra" personeli.

Sahtekarlık, kötüye kullanım veya hatalı sertifika durumu bildirimi yapacak Üçüncü Taraflar

4.9.3. Sertifika İptal Talebi Prosedürleri

"e-tuğra", sertifika iptal hizmetini, web ve çağrı merkezi üzerinden kesintisiz olarak haftada 7 gün 24 saat ilkesine göre verir. Yazıyla gelen sertifika iptal talepleri, mesai saatleri içinde işleme alınır.

"NES" iptal talepleri, sertifika sahibinden, 7 gün 24 saat ilkesine göre "e-tuğra" web sitesi üzerindeki interaktif işlemler üzerinden, çağrı merkezi üzerinde, mesai saatleri içinde yazıyla (faks ya da posta aracılığıyla "e-tuğra" veya KB'lere gelen imzalı yazılar) olmak üzere farklı yollarla alınabilir.

- Sertifika sahibi, telefonla iptal başvurusunu gerçekleştirmek isterse, ilan edilen çağrı merkezi üzerinden telefon numarası ile yetkili operatörlere ulaşır. Operatör ile birlikte T.C. Kimlik Numarası, kayıtlı cep telefonu veya e-posta aracılığıyla kendisine gönderilen onay kodu ile birlikte istenilen diğer bilgileri girerek doğrulama adımlarını tamamlar. Seri numarasını bildirdiği sertifikasının askı veya iptal işlemini tamamlar.
- "NES" sahibi, sertifika iptal talebini elle atılan imzayla hazırlayacağı bir sertifika iptal talep yazısıyla da "e-tuğra"ya bildirebilir. Yazının aslı veya kopyası ulaştığında yazıdaki imza doğrulanarak sertifika sahibi ile sistemde bulunan iletişim bilgileri kullanılarak iletişime geçilir

ve kimlik doğrulama metotları kullanılarak sertifika sahibi doğrulanır ve iptal süreci tamamlanır. Sertifika sahibi ulaşılamaz ise sertifika geçici olarak askıya alınır.

- Kurumsal başvuru sahibi veya yetkilisi, sertifika iptal talebini sadece elle atılan imzayla hazırlayacağı bir sertifika iptal talep yazısıyla "e-tuğra"ya bildirir. Yazının aslı ulaştığında yazıdaki imza doğrulanarak sertifika iptal edilir. İptal talep yazısı faksla ve e-posta ortamında taranmış olarak alınmışsa, yazı aslı gelene kadar sertifika askıya alınır. İşlem sonrası iptal durumu sertifika sahibine ve kurumsal başvuru sahibine bildirilir.
- İçeriğinde kurum bilgisi de yer alan "NES" iptal talepleri, sertifika sahiplerinin yanı sıra onaylı iptal başvuruları ile ilgili kurumu temsile yetkili kişilerden de alınabilir. Yetkililerden gelen yazılı sertifika iptal talebi doğrulandıktan sonra iptal işlemi tamamlanır. İşlem sonrası iptal durumu yetkili ile sertifika sahibine bildirilir.

Üçüncü taraflar, sahtekarlık, kötüye kullanım veya hatalı sertifika durumu gibi bildirimlerini İptal amacıyla yayınlanan eposta, destek web sitesi veya Çağrı Merkezi aracılığı ile ihbarda bulunabilirler.

"e-tuğra"ya ait bir güvenlik sorunu oluşması, mevcut sertifikalarla ilgili ihbar alınması veya sertifika üretim esnasında oluşan bir hatanın fark edilmesi durumunda, "e-tuğra" sertifika iptalini başlatabilir. Bu tür sertifika iptal işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur. Gereken durumlarda, yeni sertifika üretim işlemleri ücretsiz olarak, iptal işleminden sonra başlatılır.

İptal edilmiş bir sertifika yeniden kullanılabilir hale getirilemez.

"e-tuğra"ya ait kök ve alt kök sertifikalarının iptal edilmesi durumunda, mümkün olan en kısa sürede durum tüm ilgili taraflara elektronik ortamda duyurulur. İptal edilen kök veya alt kök sertifikanın imzasını taşıyan son kullanıcı sertifikaları da iptal edilir ve kullanıcılar e-postayla bilgilendirilir.

4.9.4. Sertifika İptal Talebi Gecikme Periyodu

Sertifika iptal talepleri "e-tuğra" tarafından teknik ve ticari imkânların elverdiği en kısa süre içinde işleme alınır. Sertifika iptal talebinin onaylanmasından sonra sertifika ilk yayınlanacak "SİL"de yer alır ve bu süre 24 saati geçmez.

İptal listeleri http://crl.e-tugra.com, http://crl1.e-tugra.com adreslerinden her bir sertifika makamı için yayınlanır.

4.9.5. Sertifika İptal Talebini İşleme Süresi

"e-tuğra", kendisine çevrimiçi (7 gün 24 saat) ulaşan tüm sertifika iptal taleplerini, talebin uygun bulunması ve kimlik doğrulamanın çevrimiçi olarak tamamlanmasının ardından teknik imkânların elverdiği en kısa sürede sonuçlandırır.

Yazıyla alınan sertifika iptal talepleri mesai saatleri içinde hemen değerlendirmeye alınır ve gerekli işlemler öncelikli olarak tamamlanır.

Sertifika iptal talebinin onaylanmasından sonra sertifika ilk yayınlanacak "SİL"de yer alır.

4.9.6. İptal Durumuna İlişkin Üçüncü Kişilerin Kontrol Yükümlülüğü

Üçüncü kişiler güvenli elektronik imzaya güvenerek bir iş veya işlem yapmadan önce sertifikanın geçerlilik durumunu kontrol etmek zorundadırlar. Üçüncü kişiler sertifikanın geçerlilik durumu kontrollerini "SİL" veya "ÇSDP" aracılığıyla kontrol etmelidirler. "e-tuğra" üçüncü kişilerin "SUE", "Sİ" ve Yönetmelik ile belirtilen kontrol yükümlülüklerini yerine getirmeleri amacıyla CWA 14171 Standardına uygun güvenli elektronik imza doğrulama aracı kullanmalarını tavsiye eder.

4.9.7. Sertifika İptal Listesi (SİL) Yayınlama Sıklığı

"NES"lere ait "SİL"ler her 6 saatte bir 24 saat geçerliliğe sahip olacak şekilde, "e-tuğra" alt kök sertifikalarına ait "SİL"ler, herhangi bir alt sertifikanın iptal edilmesi anında, aksi durumda 6 ayda bir 6 ay geçerliliğe sahip olacak şekilde yayınlanır. "e-tuğra" "SİL" hizmetini 7/24 hizmet verebilecek şekilde sağlar.

SİL geçerlilik süresi konusunda tek istisna kök ve alt kök sertifikaların geçerlilik sürelerinin dolması sırasında yaşanır. SİL içinde bulunan bir sonraki güncelleme tarihinin, kök veya alt kök sertifika geçerlilik bitiş tarihini aşması halinde SİL içinde bulunan bu değer kök veya alt kök geçerlilik bitiş tarihi olarak yazılır.

4.9.8. "SİL"lerin Yayınlanma Zamanı

SİL'ler üretildikleri andan itibaren sistem tarafından en geç 10 (on) dakika içinde http://crl.e-tugra.com ve http://crl1.e-tugra.com adreslerinde yayımlanır.

4.9.9. Çevrimiçi İptal Kontrolü Erişilebilirliği

"e-tuğra" gerçek zamanlı sertifika iptal durumu kontrolü sağlayan "ÇSDP" hizmetini kesintisiz olarak sağlar. "ÇSDP" hizmeti, kullanıcı tarafında uygun yazılımların "e-tuğra" "ÇSDP" sağlayıcısına bağlanması, durum kontrolü taleplerinin yollanması ve sağlayıcının taleplere çevrimiçi olarak cevap yollaması esasıyla çalışmaktadır. "ÇSDP" sorgusuyla, o anda bir sertifikanın durumunu geçerli, askıda, iptal, süresi dolmuş şeklinde bilgi edinilir.

Sertifika sahipleri ve üçüncü kişiler "ÇSDP" hizmetinden faydalanmak için güvenli elektronik imza doğrulama aracı kullanabilirler.

"e-tuğra" "ÇSDP" hizmeti kapsamında, sorgu yapan sistemlere verilen cevaplar, "ÇSDP" cevabı imzalama amacıyla üretilmiş olan "ÇSDP" hizmet sertifikaları kullanılarak imzalanırlar. Durumu sorgulanan ve "e-tuğra" tarafından üretilmiş herhangi bir sertifika için oluşturulan cevap, bu sertifikayı imzalamış olan kök veya alt kök sertifika tarafından imzalanmış bir "ÇSDP" hizmet sertifikası kullanılarak imzalanır.

"e-tuğra", "ÇSDP" ve "SİL" yayımlama hizmetlerinin cevap verme süresinin 10 (on) saniyenin altında kalması sağlar.

4.9.10. Çevrimiçi İptal Kontrolü Gereklilikleri

Sertifika durum sorgusu yaparken, sorgulama için ÇSDP'nü öncelikli olarak tercih etmeleri önerilir.

4.9.11. İptal Duyurularının Diğer Biçimlerine Erişilebilirlik

"ÇSDP" ve "SİL" dışında iptal durumu yayımlama yöntemi kullanmaz.

4.9.12. Anahtar Güvenliğinin Yitirilmesine İlişkin Özel Gereklilikler

Tüm Sertifikalar için, "e-tuğra", bir Özel Anahtarın güvenliğinin ihlal edildiğini tespit ederse veya bundan şüphelenirse, Güvenen Tarafları bilgilendirmek için ticari olarak makul çabayı gösterecektir. "e-tuğra", böyle bir nedenin ortaya çıkması üzerine SİL'de "anahtar ihlali" değerini kullanacaktır.

Anahtar İçerik için "e-tuğra"'ya gönderilen raporlar şunları içerir:

- Özel anahtarın kendisi.

• Sorun raporunuzun onayının ve ilgili sertifika iptallerinin gönderilmesi için geçerli bir e-posta adresi.

"e-tuğra", https://hepdesk.e-tugra.com.tr/ web sitesinde ve bu "SUE"un 1.5.2 bölümünde belirtilen diğer kaynaklarda Anahtar uzlaşması için özel talimatlar ve destek sağlar.

"e-tuğra" kök ve alt kök sertifikalarına ait imza oluşturma verilerinin gizliliğinin ve güvenliğinin şüphe altında olması halinde kök ve alt kök sertifikaları iptal edilebilir. Kök ve alt kök sertifikalarının iptal edilmesi halinde bu sertifikalara bağlı tüm sertifikalar iptal eder. "e-tuğra" kök ve alt kök sertifikalarının ve bunlara bağlı sertifikaların iptal edilmesi durumu sertifika sahiplerine ve üçüncü kişilere duyurulur.

"e-tuğra" son kullanıcıya ait sertifikalarda, güvenlik sorunu oluşması durumunda ilgili son kullanıcı sertifikalarını iptal eder, sertifika sahibini bilgilendirir.

"e-tuğra" kaynaklı tüm sertifika iptal işlemlerinde, iptal sonrası yeni sertifika üretim ve dağıtım işlemlerine en kısa sürede başlanılır.

4.9.13. Sertifika Askı Koşulları

Sertifika sahibi geçici bir süreyle "NES"in geçerliliğini kaldırmak isterse, bu sürece "NES"in askıya alınması denir. Askıya alma işleminin iptal işleminden farkı, iptal edilen "NES"in yeniden geçerlilik kazanmasının mümkün olmamasına rağmen askıya alınan "NES"in askı durumu kaldırılarak yeniden geçerlilik kazandırılabilmesidir. "e-tuğra" "NES" sahipleri ile ilgili sertifikayı askıya alma hak ve yetkisine sahip kişiler tarafından yapılan askıya alma talepleri karşısında "NES"i askıya alır.

"e-tuğra", bir sertifika iptal talebinin kaynağının doğrulanamadığı durumlarda doğrulama işlemi tamamlanana kadar iptal işlemi yerine ilgili sertifikaları askıya alır.

4.9.14. Kimler Askı Talebinde Bulunabilir

Bölüm 4.9.2'de belirtilen ilkeler uygulanır. Diğer sertifikalar için askı işlemi uygulanmaz.

4.9.15. Sertifika Askıya Alma Talebi Süreci

Bölüm 4.9.3'de yer alan ilkeler uygulanır.

"e-tuğra" ya ait bir güvenlik sorunu oluşması veya mevcut sertifikalarla ilgili ihbar alınması durumunda, iptal gerekliliği kesinleşene kadar ilgili sertifikalar "e-tuğra" tarafından askıya alabilir. Bu tür sertifika askıya alma işlemlerinde, sonuç ilgili sertifika kullanıcılarına e-posta yoluyla duyurulur.

Diğer sertifikalar için askı işlemi uygulanmaz. Kök ve alt kök sertifikaları için askıya alma işlemi uygulanmaz.

4.9.16. Askı Süresindeki Limitler

"NES" sahibi tarafından gerçekleştirilen askıya alma işlemi sertifika geçerlilik süresinin sonuna kadar devam edebilir.

"e-tuğra"nın, bir "NES" iptal talebinin kaynağının doğrulanamadığı durumlarda askıya aldığı sertifikalar, doğrulama işlemi sonuçlanıncaya veya süre sınırı aşılana kadar askıda bırakılır. "NES" sahipleri tarafından iptali gerektiren bir durumun olup olmadığından emin olunamadığında askıya alınan "NES"ler, "NES" sahibinden iptal gerekliliği onaylandığında iptal edilir. Bu sürenin sonunda hala askıda bulunan "NES"ler, güvenlik nedeniyle otomatik olarak iptal edilir. "NES"lerin askıda bulunduğu süre içinde, iptali gerektiren bir durumun olmadığı anlaşılırsa, "NES" askıdan çıkarılarak tekrar geçerli duruma alınabilir.

Diğer sertifikalar için askı işlemi uygulanmaz.

4.10. Sertifika Durum Hizmetleri

Sertifika durum sorgulaması 2 (iki) ayrı yöntemle yapılır: Sertifika İptal Listesi (SİL) ve Çevrimiçi Sertifika Durum Protokolü ("ÇSDP"). İptal durumu bilgileri, minimum ilgili sertifikanın geçerliliği tarihi sonuna kadar yayınlanır.

4.10.1. Operasyonel Özellikler

Sertifika durum kontrolleri "SİL"ler ve "ÇSDP" aracılığıyla yapılır. "e-tuğra" "SİL" ve "ÇSDP" hizmetlerini 7/24 kesintisiz aşağıdaki adreslerden sağlar.

- http://crl.e-tugra.com
- http://crl1.e-tugra.com
- http://ocsp.e-tugra.com veya
- http://ocspvn.e-tugra.com

4.10.2. Hizmetin Sürekliliği/Erişebilirliği

"e-tuğra", "SİL" ve "ÇSDP" hizmetini, kesintisiz olarak 7 gün 24 saat ilkesine göre verir. Bu hizmetler 1 saatten daha fazla erişme kapalı olamaz.

"SİL" hizmeti fiziksel olarak da farklı bir noktadan ikinci bir sunucu üzerinden de verir.

"ÇSDP" hizmetinin kesintiye uğramasını engellemek için, "e-tuğra" merkezinde sunulan sertifika hizmetleri, erişilebilirlik ve yeniden devreye alma amaçları uyarınca her zaman yeterli düzeyde bir Felaket Kurtarma Merkezi ile idame ettirilir. Hizmetlerinin "e-tuğra"nın kontrolü dışında aksaması halinde, "e-tuğra" en kısa süre süre içerisinde hizmetlerin tekrar sağlanabilmesi için Felaket Kurtarma Merkezi'ni devreye alır.

4.10.3. İsteğe Bağlı Özellikler

İlgili değildir.

4.11. Sertifika Sahipliğinin Sona Ermesi

Geçerlilik süresi dolan ve iptal edilen sertifikalar için sertifika sahipliği sona erer.

4.12. İmza Oluşturma Verisi Kurtarma ve Yedekleme

"e-tuğra", sertifika sahiplerinin imza oluşturma verilerini hiçbir biçimde yedeklemez, yeniden oluşturmaz; yeniden oluşturulabileceği bilgileri elinde tutmaz ve kurtarma hizmeti vermez..

4.12.1. İmza Oluşturma Verisi Kurtarma ve Yedekleme İlke ve Esasları

İlgili değildir.

4.12.2. Oturum Anahtarı Zarflama ve Kurtarma İlke ve Uygulamaları

İlgili değildir.

5. TESİS, YÖNETİM VE OPERASYONEL KONTROLLER

Bu bölümde “e-tuğra”nın “ESHS” olarak sertifika hizmetlerini yürütürken uyguladığı temel fiziksel ve operasyonel kontroller ve prosedürler açıklanmaktadır.

5.1. Fiziksel Kontroller

5.1.1. Tesis Konumu ve İnşası

“e-tuğra”, sertifika yaşam zinciri operasyonları ve anahtar yönetimi de dahil olmak üzere temel "ESHS" operasyonlarının tümünü gizli veya açık müdahaleleri durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan, içerisinde çeşitli güvenlik alanları oluşturulmuş bir “Güven Merkezi” içinde yürütür.

5.1.2. Fiziksel Erişim

“e-tuğra” “Güven Merkezi”ndeki alanlara fiziksel erişim sürekli kontrol altında tutulmaktadır.

5.1.3. Güç Kaynakları ve Havalandırma

“Güven Merkezi” ve “e-tuğra”nın temel “ESHS” operasyonlarında kullanılan donanımların, 7/24 operasyonlarına devam edebilmeleri için kesintisiz güç kaynakları ve jeneratör ile; sıcaklığı ve nispi nemi kontrol etmek için ise ısıtma/havalandırma/klima sistemleri ile donatılmıştır.

5.1.4. Suya Karşı Korunma

“e-tuğra” “Güven Merkezi” su baskınları ve sele karşı koruma altındadır.

5.1.5. Yangın Önlemleri ve Korunması

“e-tuğra”, yangınları veya hasara yol açan diğer alev veya duman vakalarını önlemek ve söndürmek için gerekli tüm önlemleri almıştır.

5.1.6. Veri Araçları Saklanması Ortamları

Üretimde kullanılan yazılım ve veriler ile denetim, arşiv veya yedekleme bilgilerini içeren bütün araçlar “Güven Merkezi”nde veya erişimi yetkili kişilerle sınırlandırılarak ve araçları kazayla hasara (örneğin, su, yangın ve elektromanyetik) karşı koruyacak şekilde tasarlanarak, uygun fiziksel erişim kontrollerine sahip güvenli ortamlarda muhafaza edilir.

5.1.7. Atık Kontrolü

Sertifika yaşam zinciri hizmetlerinde ve “e-tuğra”nın diğer “ESHS” operasyonlarında kullanılan ve geçerliliğini ve/veya gerekliliğini yitiren tüm dokümanlar ve elektronik veriler bu amaçla hazırlanan ilgili süreçler doğrultusunda imha edilir. “e-tuğra”nın kendisine ait güvenli elektronik imza oluşturma araçları ve ilgili diğer kriptografik donanım fiziksel olarak imha edilir veya üretici firmanın talimatları doğrultusunda sıfırlanır; diğer tüm atıklar normal süreçlerle bina dışına çıkarılır.

5.1.8. Harici Alan Yedeklemesi

“e-tuğra” olası teknik arızalara ve/veya afetlere karşı, sertifika yönetim süreçleri iş sürekliliğini sağlamak amacıyla “İş Sürekliliği Planı” ve “Felaketten Kurtarma Planı” doğrultusunda “Güven Merkezi” içinde ve dışında rutin olarak elektronik kayıtların yedeklerini alır ve saklar.

5.2. Prosedür Kontrolleri

5.2.1. Güvenli Roller

Sertifika yaşam zinciri ve elektronik sertifika hizmetleri, anahtar yönetimi kontrolleri, “e-tuğra” yönetim sistemleri ve veri bankaları kontrolleri, gerekli erişim ve kontrol yetkisine sahip “güvenli personel” tarafından yürütülür. “Güvenli personel”, “AAA” teknolojisi, bilgi güvenliği ve risk yönetimi konularında yeterli bilgi ve tecrübe seviyesine sahip kişilerden seçilir. “e-tuğra” “Güvenli personel” tanımları aşağıdaki şekildedir;

- **Üst Düzey Yöneticiler:** “e-tuğra” sertifika hizmetlerinin yürütülmesinden teknik ve idari açıdan sorumlu üst düzey yöneticilerdir.
- **Güvenlik Yöneticileri**: Güvenlik sisteminin tüm politika ve prensiplerinin belirlenmesi, uygulanması, onaylanması görev, yetki ve sorumluluğuna sahip “güvenli personel”.
- **Trust Center Yöneticisi:** Güvenlik uygulamalarının yönetimine ilişkin tüm teknik sorumluluğa sahip “güvenli personel”.
- **Sertifika Operatörü:** Başvuru evrak kontrolü, sertifika başvuru kaydı, üretim, “NES”lerin oluşturulması, iptali, askıya alınması gibi operasyonel konularda görev ve yetkiye sahip “güvenli personel”.
- **Kayıt Birimi (KB) İşletmeni:** Başvuru evrak kontrolü, sertifika başvuru kaydı, iptal, askı taleplerinin alınması gibi operasyonel konularda görev ve yetkiye sahip “güvenli personel”.
- **Sistem Yöneticileri (Ağ ve Sistem Yöneticisi):** Sertifika hizmetleri ve yönetimi için kullanılan “e-tuğra” “ESHS” güvenli sistemlerini kurma, konfigüre etme ve bakımını yapma görev ve yetkisine sahip “güvenli personel”dir. Aynı zamanda, “e-tuğra” “ESHS” güvenli sistemlerini günlük bazda kullanma, sistem yedeklemesi ve kurtarma fonksiyonlarını kullanma görev ve yetkisine sahiptirler.
- **Sistem Denetçileri:** “e-tuğra” “ESHS” güvenli sistemlerinin denetim kayıtlarına ve arşivlerine erişme ve devamlılığını sağlama görev ve yetkisine sahip “güvenli personel”

“Güvenli personel” Bölüm 5.3’deki kriterleri yerine getiren kimseler arasından ve güvenlik açısından tam yetkili bir yönetici tarafından seçilir ve görevlendirilir.

5.2.2. Her Bir Görev için Gereken Kişi Sayısı

“e-tuğra”nın kritik operasyonel prosedürleri hazırlanan talimatlar çerçevesinde genel olarak birden fazla “güvenli personel”in katılımıyla gerçekleştirilmektedir. Kritik operasyonel prosedürler, kriptografik araç kullanımı gerektiren yüksek güvenlik gereksinimi olan uygulamalardır.

“e-tuğra” "ESHS" kök ve alt kök sertifikasına ilişkin oluşturma, yenileme ve iptal işlemleri, en az ikisi yönetici seviyesindeki “güvenli personel” olmak üzere gerekli nitelik ve yetkilere sahip birden çok kişinin katılımıyla gerçekleştirilir.

5.2.3. Her Bir Görev için Tanımlama ve Kimlik Kontrolü

"Güvenli personel" olarak seçilen kimseler gerekli kimlik ve biyolojik bilgileri alınarak kendilerine atanan yetkiler doğrultusunda güvenlik sistemine kaydedilir. Kritik operasyonel işlemler öncesinde, işlemle ilgili yetki kontrolü ve görevli tanımlaması yapılır; yetki kontrolü ve tanımlamanın başarılı olması halinde işleme izin verilir ve kayıt altına alınır.

5.2.4. Sorumlukların Ayrılmasını Gerektiren Roller

Sertifika yaşam zinciri işlemleri, "ESHS" anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok "güvenli personel"in katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilir. Sorumlulukların ayrıştırılması prensibi ile bir işlemin tümünün veya büyük bir kısmının tek bir kişi tarafından yapılması engellenmiştir. Yapılan her işlem tarih, rol ve işlemi gerçekleştiren personel bazında kayıt altına alınır.

5.3. Personel Kontrolleri

5.3.1. Nitelik, Deneyim ve Güvenlik Gereklilikleri

"e-tuğra" istihdam politikası, "e-tuğra" "ESHS" gereksinimleri göz önünde bulundurularak oluşturulmuştur. İstihdam politikası genel personel istihdamı ve "güvenli personel" istihdamı olarak ikiye ayrılmaktadır. "e-tuğra" genel personeli, "Güven Merkezi" operasyonlarında görev almayan, pazarlama, organizasyon ve belirli idari görevlerde yer alan personelden oluşur. Tüm personel alımlarında ve görevlendirmelerinde, personel güvenlik kontrollerinden geçirilir.

"e-tuğra" genel personeli işe alımı, üst düzey bir yönetici tarafından personel adayının gerekli niteliklere sahip olduğuna, uygun eğitime sahip olduğuna ve sır saklama yükümlülüğünü taşıyabileceğine kanaat getirildikten sonra gerçekleştirilir.

5.3.2. Mesleki Bilgi Kontrol Prosedürleri

"e-tuğra" genel personeli ve "güvenli personeli" hakkında işe alımdan önce referansların değerlendirilmesi, önceki işin kontrolü, eğitim bilgilerinin ve niteliklerinin doğrulanması, ise teknik ve idari açıdan uygunluğu, adli sicil kontrolünü de içeren bir dizi güvenlik ve tanımlama kontrolleri yapılır.

5.3.3. Eğitim Gereksinimleri

e-Tuğra" personeli göreve başlamadan önce "ESHS" hizmetleri, sertifika yaşam zinciri hizmetleri, mesleki sorumluluklar, temel açık anahtar altyapısı çerçevesi, Kayıt Birimi ve "Güven Merkezi" işleyişi, "e-tuğra" güvenlik prosedürleri, sertifika politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler. "e-tuğra" eğitim programları periyodik olarak gözden geçirilir ve gerekli görüldüğünde güncellenir.

5.3.4. Eğitim Sıklığı ve Şartları

"e-tuğra", personeline, ilk eğitimleri haricinde belirli aralıklarla ve güncellenmiş içeriklerle eğitim verilir. Kurum içerisinde yapılan performans analizleri doğrultusunda eğitim sıklığı ve içeriği değiştirilebilir. "e-tuğra" operasyonlarında veya kullanılan yazılım ve donanımlar da değişiklik veya güncelleme olduğunda ve gerekli görüldüğü takdirde eğitimler düzenlenebilir.

5.3.5. İş Rotasyon Sıklığı ve Sırası

"e-tuğra" yönetimi gerekli ve uygun gördüğü durumlarda personelin, bilgi, beceri ve tecrübesine bağlı olarak rotasyona tabi tutabilir.

5.3.6. Yetkisiz Eylemlere Karşı Yaptırımlar

"e-tuğra" güvenlik ve işleyiş politikalarının personel tarafından ihlali halinde "e-tuğra" tarafından personel hakkında gerekli disiplin önlemleri alınır ve personel ile yapılan gizlilik sözleşmelerindeki cezai şartlar yürürlüğe konulur. Söz konusu ihlaller sebebiyle "e-tuğra" veya hizmet sağladığı kimseler herhangi bir şekilde zarar görürse "e-tuğra" sorumlu personele zararı tazmin ettirebilir.

Yetkisiz eylemler veya süreç ihlali fiilleri Elektronik İmza Kanunu, Türk Ceza Kanunu ve ilgili diğer kanunlarda belirtilen suç tanımlarına dahil olması durumunda bu eylemleri gerçekleştirenler hakkında gerekli yasal işlemler yapılır.

5.3.7. Bağımsız Yüklenici İsterleri

"e-tuğra", "ESHS" faaliyetlerini yürütmek için bağımsız yükleniciler ile hizmet sözleşmeleri akdedebilir. Hizmet sözleşmeleri "e-tuğra"nın güvenlik ve işleyiş süreçlerine uyumlu olacak şekilde düzenlenir.

5.3.8. Personele Verilen Dökümanlar

"e-tuğra" tüm personeline "SUE", "Sİ" dökümanları, sertifika hizmetleri ile ilgili prosedürler ve güvenlik prosedürleri ile talimatları, çalışanların rollerine göre düzenlenmiş görevleriyle ilgili özel nitelikli yazılım ve donanım kullanım kılavuzlarını verir.

5.4. Denetim ve Kayıt Prosedürleri

5.4.1. Kaydedilen Olay Tipleri

Sertifika yaşam döngüsü içinde yürütülen tüm sertifika hizmetlerine ait kayıtlar tutulur. "e-tuğra"nın "ESHS" işleyişine ve organizasyonel fonksiyonlarına ilişkin aşağıdaki kayıtlar elektronik ve/veya kağıt ortamında olayın tanımı, gerçekleşme tarihi, olayla ilgili kişilere ilişkin bilgiler de dahil olmak üzere tutulur.

- "ESHS" anahtar (veri) yaratma, yedekleme, saklama, kurtarma, arşivleme ve imha etme.
- Sertifika başvuruları, yenileme, yeniden anahtarlama, askı ve iptal işlemleri.
- Sertifikaların ve "SİL"lerin yaratılması ve yayınlanması.
- Başarılı veya başarısız sisteme erişim girişimleri.
- Sistem arızaları, donanım arızaları ve diğer anormallikler.
- Personelin "Güven Merkezi"ne giriş çıkış kayıtları.
- Güvenlik duvarı ve router aktivitesi.
- "ESHS" ana merkezi tesisi ziyaretçi girişi/çıkışı

5.4.2. Kayıt İşleme Sıklığı

Denetim kayıtları sürekli olarak tutulur ve belirli zaman aralıklarıyla incelenir. Denetim kayıtları belirli aralıklarla yedeklenir ve arşivlenir.

5.4.3. Denetim Kaydı Saklama Süresi

Denetim kayıtları işlendikten sonra veri depolama kapasitesine göre erişilebilir şekilde sistemde tutulur. İlgili mevzuata göre saklanması gereken bilgi ve belgeler ise bölüm 5.5.2'ye göre arşivlenir.

5.4.4. Denetim Kaydının Korunması

Elektronik ve kağıt ortamındaki denetim kaydı dosyalarına, yetkisiz kişilerin izlemesine, değişiklikler yapmasına, silmesine veya başka herhangi bir şekilde erişmesine karşı fiziksel ve mantıksal erişim kontrolleri kullanılır ve bu yolla denetim kaydı dosyaları korunur.

5.4.5. Denetim Kaydı Yedekleme Prosedürleri

Denetim kayıtları ilgili arşivleme süreçleri doğrultusunda periyodik olarak "Güven Merkez" içinde ve dışında yedeklenir.

5.4.6. Denetim Bilgisi Toplama Sistemi

Başvuru safhasında, ağ ve işletim sistemi seviyesinde, elektronik ortamda gerçekleşen işlemlerin denetim verileri "ESHS" yönetim uygulaması tarafından otomatik olarak oluşturulur ve kaydedilir. Manuel olarak yapılan işlemlere ilişkin denetim verileri "e-tuğra" personelince manuel olarak kaydedilir.

5.4.7. Olaya Sebep Olan İlgiliye Bilgilendirme

Denetim bilgisi toplama sistemi önemli bir olay kaydettiği zaman, olaya sebep olan birey, kurum veya görevliye ihbarda bulunmaya gerek yoktur. Ancak olayın niteliğine ve önem derecesine göre sistem kişinin yönetiminden sorumlu üst yetki seviyesindeki kişi veya kişileri bilgilendirir.

5.4.8. Güvenlik Açıklarının Değerlendirilmesi

Denetim kayıtlarının rutin olarak gözden geçirilmesi sonucunda sistemdeki ve süreçlerdeki güvenlik açıkları tespit edilerek gerekli olan önlemler alınır.

5.5. Kayıtların Arşivlenmesi

5.5.1. Arşivlenen Kayıt Tipleri

Aşağıda listelenen belge ve bilgiler "e-tuğra" arşiv prosedürleri uyarınca yedeklenir ve arşivlenir.

- Sertifika süreçlerine yönelik tüm başvurular, başvuru sözleşmeleri, ilgili diğer sözleşme ve belgeler.
- Sertifikaların oluşturulması, iptali, askıya alınması ve yenilenmesiyle ilgili eylem ve bilgiler (eylemlerin zamanı ve eylemleri yapan yetkililer de dahil olmak üzere).
- Müşteriler ve iş ortaklarıyla yapılan sözleşmeler, önemli yazışmalar.
- Bölüm 5.4'de belirtilen tüm denetim kayıtları.
- Tüm sertifikalar ve "SİL"ler.
- Geçerlilik süresinin sona ermesinden itibaren "ESHS" kök ve alt kök sertifikası.

- İptal, askıya alma, askıdan kaldırma ile ilgili talep ve talebin doğrulanması eylemleri ve ilgili iletişim bilgileri.
- "e-tuğra" tarafından yayınlanan bütün "SUE", "Sİ" belgeleri (yayınlanmış bütün sürümleri).
- "e-tuğra" tarafından kullanılan tüm prosedürler, talimatlar ve hazırlanan formlar.

5.5.2. Arşiv Saklama Periyodu

"Yönetmelik" ve ilgili mevzuat hükümleri doğrultusunda Bölüm 5.5.1'de belirtilen kayıtlar en az 20 yıl süreyle saklanır.

5.5.3. Arşivin Korunması

Elektronik olarak arşivlenmiş veriler, uygun fiziksel ve mantıksal erişim kontrolleri kullanılarak, yetkisiz izleme, değiştirme, silme veya başka herhangi bir şekilde erişime karşı korunur.

Manuel olarak girilen kâğıt ortamındaki bilgiler ise sadece yetkililerin erişebildiği fiziksel korumalı alanlarda saklanır.

5.5.4. Arşiv Yedekleme Prosedürleri

"e-tuğra" gerekli gördüğü bilgi ve belgelerin yedeklerini, orijinalleriyle aynı güvenlik seviyesinde olmak şartıyla "Güven Merkezi" içinde ve/veya dışında tutabilir.

Kâğıt ortamındaki arşivlerin yedekleri alınmaz.

5.5.5. Kayıtlara Zaman Damgası Basma Şartları

SİL'ler, diğer iptal veritabanı girdileri ve "e-tuğra" tarafından gerekli görülen diğer bilgi ve belgeler tarih bilgisi içerir; kullanılan tarih bilgisi zamanı UTC ile senkronize edilir. Gerekli görülen kayıtlara zaman damgası basılır.

5.5.6. Arşiv Toplama Sistemi

Arşivler "e-tuğra" yönetim sistemleri kullanılarak elektronik ortamda veya yetkili kişilerin sorumluluğunda manuel olarak toplanır.

5.5.7. Arşiv Bilgisine Ulaşma ve Doğrulama Prosedürleri

"SUE", "Sİ" dokümanları ile son kullanıcı sözleşme örnekleri web sitesinin ilgili bölümünde (bilgi deposu) yayınlanır. Gizli belgelere ise sadece "güvenli personel" ve Bilgi Teknolojileri ve İletişim Kurumu yetkilileri tarafından erişilebilecektir. Sertifika başvuruları ve sertifika sahiplerine ilişkin kimlik bilgileri ve diğer bilgilere ise sadece kendisiyle ilgisi olmak şart ve koşuluyla kurumsal başvuru yetkilileri, "güvenli personel", kayıt işlemlerinden sorumlu yetkililer ve Bilgi Teknolojileri ve İletişim Kurumu yetkilileri tarafından erişilebilecektir.

5.6. Anahtar (İmza Oluşturma – Doğrulama Verileri) Değiştirme

"e-tuğra" "ESHS" kök ve alt kök sertifikalarının geçerlilik süreleri, ilgili mevzuatta belirtildiği üzere, en fazla 10 yıl olacaktır. Gerekli görülen durumlarda güvenlik sebebiyle ve kök ve alt kök sertifikalarının geçerlilik süresinin dolmasından önce sertifikalar yenilenebilir. ECSP hizmetlerinin devamlılığı için, yeni "ECSP" kök ve alt anahtar çiftleri ve sertifikaları, mevcut kök ve alt sertifikaların sona erme tarihinden en az 4 yıl önce oluşturulur. Eski anahtarlar geçerlilik süresinin sonuna kadar kullanılabilir durumda

saklanır. “ESHS”nin kök ve alt kök sertifikalarının değişiminden itibaren yeni oluşturulacak sertifikalar yeni yeni alt kök sertifikalar ile imzalanır. Ancak eskiden oluşturulmuş olan sertifikaların doğrulanabilmesi için önceki “e-tuğra” “ESHS” kök sertifikası ve alt kök sertifikalarına erişilebilirliği sağlanır.

5.7. Tehlike ve Felaketten Kurtarma

5.7.1. Olayları ve Tehlikeleri Kontrol Altında Tutma Prosedürleri

“ESHS” işleyişinin güvenilirliğini etkileyecek nitelikte olayların oluşması durumunda “İş Sürekliliği Planı”, “Felaketten Kurtarma Planı” ve diğer bilgi güvenliği yönetim sistemi prosedürleri doğrultusunda sistemin en kısa sürede güvenli bir şekilde işler hale gelmesi, etkilenen taraflara haber verilmesi ve diğer önlemlerin uygulanması için gerekli önlemler alınır.

5.7.2. Donanım, Yazılım ve/veya Veri Bozulması

“Güven Merkezi”nde bulunan donanım, yazılım ve gerekli verilerin bozulması halinde öncelikle yedek donanım ve yazılım faaliyete geçirilir. “İş Sürekliliği Planı” ve “Felaket Kurtarma Planı” doğrultusunda kaybolan verilerin yedekleri işleme konulur ve/veya yeniden oluşturulur. Kurtarılamayan veriler sebebiyle sertifika yönetim süreçlerinde geri dönülemez arızalar meydana gelmesi halinde, arızadan etkilenen sertifikalar derhal iptal edilir ve yeni sertifika üretimine geçilerek ilgili taraflara bilgi verilir.

5.7.3. İmza Oluşturma Verisinin Zarar Görmesi

“e-tuğra” “ESHS” kök sertifikalarının imza oluşturma verilerinin güvenliğinin tehlikeye düşmesi durumunda “İş Sürekliliği Planı” ve Felaket Kurtarma Planı” doğrultusunda ilgili tüm sertifikalar derhal iptal edilir ve ilgili tüm taraflar web sitesi ve e-posta aracılığıyla haberdar edilir. “e-tuğra” “ESHS” kök sertifikalarının yeni imza oluşturma verilerini oluşturur.

5.7.4. Felaket Sonrası İş Sürekliliği

“e-tuğra”, “İş Sürekliliği Planı” ve “Felaket Kurtarma Planı” doğrultusunda işleyişi engelleyecek olaylar karşısında ortaya konacak eylem ve işlemler belirlenir.

5.8. “e-tuğra”nın Operasyonunun Durdurulması

“e-tuğra” faaliyetlerinin son bulması mecburiyeti halinde, ilgili “Kanun” ve “Yönetmelik” gereği bu durumu en az 3 ay önce Bilgi Teknolojileri ve İletişim Kurumu ‘na bildirir ve kamuoyuna duyurur. Prosedürler uyarınca, mevcut “NES”ler ilgili tüm bilgi, belge ve kayıtları, Kanun gereği bir ay içinde anlaştığı veya kurumun re’sen belirlediği mevcut bir "ESHS"ye devreder. Bilgi Teknolojileri ve İletişim Kurumu gerekli ve uygun görmesi halinde, bir ayı geçmemek üzere ek süre verebilir.

Eğer devir işlemi belirtilen süreler içinde tamamlanmazsa, “e-tuğra” ilgili sertifikaları iptal eder ve tüm ilgili tarafları genel duyuru ile; sertifika sahiplerini ve kurumsal başvuru sahiplerini ise doğrudan e-posta aracılığıyla haberdar eder. Bu durumda, tüm iptaller tamamlandıktan ve “SİL” kaydı oluşturduktan sonra kendi imza oluşturma verisi ile yedeklerini imha eder.

Tüm sertifika sahipleri de yukarıda kamuoyuna yapılan duyuruyla ve e-postayla faaliyetin son bulmasından haberdar olmuş olurlar. “NES”ler için zorunlu olarak yapılan devir işlemi bu sertifikalar için de yapılmaya çalışılır.

Bu maddedeki tüm hükümler sadece aktif olan taraflar için geçerlidir.

6. TEKNİK GÜVENLİK KONTROLLERİ

6.1. Anahtar Çifti Üretimi ve Kurulumu

6.1.1. Anahtar Çifti Üretimi

“e-tuğra” kök ve alt kök sertifikalarına ait anahtar çifti verilerini oluşturma işlemi, oluşturulan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş en az iki eğitimli “güvenli personel” ve ilgili görevliler tarafından , Bölüm 5.2.2’de belirtildiği şekilde teknik ve idari güvenlik önlemleri alınmış ortamlarda ilgili prosedürlere uygun olarak yerine getirilir. “e-tuğra” kök sertifikası için, imza oluşturma ve doğrulama verileri oluşturmada kullanılan şifreleme modülleri FIPS 140-1 Seviye 3 şartlarını karşılar. “e-tuğra” kök sertifikasının imza oluşturma ve doğrulama verileri “Tebliğ”de belirtilen algoritmalara ve ETSI EN 319 411-1 dokümanlarına uygun olarak oluşturulur; anahtar oluşturma işlemi sırasında yapılan faaliyetler tüm detayları ile kaydedilir, tarih atılarak imzalanır. Bu kayıtlar denetim ve izleme amacıyla saklanır. Anahtar çiftleri “ESHS”nin güvenli elektronik imza oluşturma aracında oluşturulur ve buradan yedekleme amacı dışında çıkarılamaz. İmza oluşturma verisinin güvenli olarak saklanması için gerekli fiziksel ve teknik güvenlik önlemleri alınır.

“e-tuğra” kök sertifikasının imza oluşturma ve doğrulama verileri Türkiye Cumhuriyeti sınırları içerisinde oluşturulur ve imza oluşturma verisi hiçbir şekilde bu sınırlar dışına çıkarılamaz. “e-tuğra” kök sertifikasının, imza oluşturma ve doğrulama verilerinin geçerlilik süresi 10 yılı aşamaz.

“e-tuğra” donanım güvenlik modülleri, fiziksel ve elektronik her türlü müdahaleye karşı koruma altında tutulur ve çalıştırılır. Modüllerde bulunan verinin güvenli yedekleri ilgili prosedürlere göre alınır ve saklanır. Fiziksel olarak değiştirilmesi gereken bir modülün içindeki anahtarlar Bölüm 6.2.10’da belirtildiği gibi yok edilir ve yeni modüllerde kullanılmak üzere gerekli yedekler başka ortamlarda saklanır.

“e-tuğra” “ESHS” iş modeline göre “Sertifika Sahibi”ne ait olan imza oluşturma ve doğrulama verileri “Tebliğ”in 6. Maddesinde belirtilen algoritma ve parametrelere uygun olarak “Sertifika Sahibi” adına “ESHS”ye ait olan yerlerde “e-tuğra” tarafından oluşturulacaktır. İmza oluşturma verisi güvenli erişim sağlayan yazılımlar ile “güvenli personel” tarafından ISO/IEC 15408 (-1,-2,-3)’e göre en az EAL 4+ güvenlik standardına sahip bir güvenli elektronik imza oluşturma aracı içerisinde oluşturulur. “e-tuğra” “Sertifika Sahibi”ne ait olan imza oluşturma verilerinin bir kopyasını almaz ve/veya imza oluşturma verileri “e-tuğra” tarafında saklanmaz.

6.1.2. Sertifika Sahibine İmza Oluşturma Verisinin Verilmesi

İmza oluşturma verileri sertifika sahiplerine “NES” ile birlikte güvenli elektronik imza oluşturma aracı içerisinde üretilir ve verilir. Asgari “Güvenli Elektronik İmza Oluşturma Aracı” ve bu araç içerisinde bulunan imza oluşturma ve doğrulama verileri ve “NES”in bulunduğu “Güvenli e-imza Paketi” “NES” sahibine kimlik kontrolü ve imza karşılığında, kargoyla; “e-tuğra” merkezinde doğrudan kendisine veya KB yetkilisi tarafından yine doğrudan kendisine teslim edilir. Güvenli elektronik imza oluşturma aracının kullanılabilmesi için gereken erişim verisi de çağrı merkezi veya güvenli kargo aracılığıyla veya e-tuğra web sitesi üzerinden interaktif işlemler aracılığı ile “NES” sahibine iletilir.

6.1.3. İmza Doğrulama Verisinin "ESHS"ye Ulaştırılması

Anahtar çiftleri imza oluşturma aracı içerisinde üretilir ve gizli anahtar “e-tuğra” tarafından saklanmaz.

Anahtar üretiminin sertifika başvuru sahibi tarafından gerçekleştirildiği durumlarda, sertifika talebinin gizli anahtarla imzalanmış olması şarttır. Talep bilgisinin güvenliğini ve üçüncü kişilerin erişimini engellemek için, talebin güvenli elektronik haberleşme yoluyla "e-tuğra"ya ulaşması sağlanır.

6.1.4. Kullanıcılara "ESHS" İmza Doğrulama Verilerinin Verilmesi

"e-tuğra" "ESHS" sertifikaları (kök ve alt kök sertifikalar http://www.e-tugra.com.tr/crt adresinde yayınlanır. Bu sertifikalara ait SHA-1 özeti Türkiye'de yayımlanan en yüksek tirajlı üç ulusal gazetede kamuoyuna duyurulur.

6.1.5. Anahtar Uzunlukları

"e-tuğra" kök sertifikaları 4096 bit RSA, alt kök sertifikaları 2048 bit RSA anahtar çiftleri kullanılarak üretilir.

Alt kök sertifikaları ve "NES", Tebliğ'le belirlenen minimum anahtar uzunlukları dikkate alınarak üretilir.

Sertifikalarda kullanılan özetleme algoritmaları hakkında Bölüm 7.1.3'te bilgi verilmiştir.

6.1.6. Anahtar Üretim Parametreleri ve Kalite Kontrolü

"e-tuğra" kök sertifikalarına ait anahtarlar ve "NES" anahtarları "e-tuğra" "Güven Merkezi"nde veya yetki verilmiş "Kayıt Birim"lerinde fiziksel ve teknik güvenlik şartları sağlanmış olarak, "güvenli personel" tarafından oluşturulur. Oluşturma sırasında kullanılan parametreler, algoritmalar ve araçlar "Tebliğ" ile belirtilen gerekliliklere uygundur.

6.1.7. Anahtar Kullanım Amaçları

"e-tuğra" tarafından üretilen kullanıcı sertifikaları sadece güvenli elektronik imza ve kimlik doğrulama amacıyla kullanılır.

"e-tuğra" kök sertifikası anahtarları ise kullanıcı sertifikalarını imzalama, "SİL" imzalama, "ÇSDP" sertifikası imzalama, zaman damgası sertifikası imzalama amaçlarıyla kullanılabilirler. Anahtarların kullanım amaçları, sertifikaların anahtar kullanım alanlarında belirtilir.

6.2. İmza Oluşturma Verisinin Korunması ve Şifreleme Modülü Sistem Kontrolleri

6.2.1. Kriptografik Modülü Standartları ve Kontrolleri

"NES"lerin imza oluşturma ve doğrulama verilerini oluşturmak için ve "SİL" imzalama işlemleri için "Tebliğ"de belirtilen standartlara uygun güvenli elektronik imza oluşturma araçları kullanılır.

"e-tuğra" kök sertifikasının imza oluşturma, doğrulama verileri oluşturma ve imza oluşturma verisi saklama işlemleri için FIPS 140-1 Seviye 3'de yetkili onaylanmış donanım şifreleme modülleri kullanılır.

Modüllerin tüm kullanım ömürleri boyunca, cihazlar işlevsellikleri ile ilgili sürekli kontrol altında tutulur ve herhangi bir güvenlik ihlali durumu ilgili prosedür uyarınca yönetilir.

Güvenli elektronik imza oluşturma araçlarındaki imza oluşturma verilerinin dışarıya çıkarılması, değiştirilmesi veya kopyalanması engellenmektedir.

6.2.2. İmza Oluşturma Verisi (n* m) Çok Kullanıcılı Kontrolü

"e-tuğra" "ESHS" imza oluşturma ve doğrulama verilerine erişim ancak birden çok yetkili "güvenli personel"in gerekli güvenlik ve tanımlama prosedürlerini yerine getirmesi ile gerçekleştirilmektedir.

Fiziksel ve sistemsel erişim kontrollerinin yanı sıra, bu imza oluşturma verilerinin kullanımı, en iki farklı güvenli roldeki personelin onayı ile mümkündür.

Kök ve alt kök sertifikalarının gizli anahtarlarının bulunduğu kriptografik modüllere erişim ve anahtarların kullanılması erişim şifrelerine sahip iki yetkilinin aynı anda bulunmasıyla mümkündür.

"NES" imza oluşturma verileri sorumluluğu sadece sertifika sahiplerine aittir ve şifre kontrollü güvenli elektronik imza oluşturma araçlarında saklanır.

6.2.3. İmza Oluşturma Verisinin Saklanması

"e-tuğra", "ESHS" imza oluşturma verisini, resmi makamların erişimi amacıyla dahi olsa herhangi bir üçüncü şahsa vermez. "e-tuğra", sertifika sahiplerine ait imza oluşturma verilerinin kopyalarını hiçbir şekil ve şartta almaz ve saklamaz.

6.2.4. İmza Oluşturma Verisi Yedekleme

"e-tuğra", rutin ve felaketten kurtarma amaçlarıyla "ESHS" imza oluşturma verilerinin yedek kopyalarını oluşturur. Bu veriler, donanım şifreleme modüllerinde ve ilgili anahtar saklama cihazlarında gerekli teknik ve fiziksel güvenlik önlemleri alınarak, EAL4+ veya FIPS 140-2 Düzey 3 sertifikalı güvenli donanımlarda anahtar üretim ve yedekleme prosedürlerine uygun şifrelenmiş formda oluşturulur. Bu yedekler, "Güven Merkezi" dışında farklı güvenli kasalarda saklanır.

Yedeklerin kullanım ihtiyacı oluşması durumunda, yedek gizli anahtarların ilgili donanım güvenlik modüllerine geri yüklenmesi için, "e-tuğra" imza yetkilisi yedekleri "Güven Merkezi"ne getirir ve bu yedekler sadece yetkili kişiler tarafından kullanılır. Gizli anahtarların yedekleme ve yeniden kullanım işlemleri, en az iki yetkili personelin aynı anda hazır bulunmasıyla, teknik ve idari güvenliği sağlanmış alanlarda ve gerekli erişim bilgileri girilmesi ile yürütülür.

Tüm son kullanıcılara ait imza oluşturma verileri yedeklenmez.

6.2.5. İmza Oluşturma Verisi Arşivleme

"e-tuğra" "ESHS" kök sertifikalarına ait imza oluşturma verileri arşivlenmez, imza doğrulama verileri ve kök sertifikalar ise ileride çıkması muhtemel uyuşmazlıklarda kullanılmak üzere 20 yıl süreyle saklanır. "e-tuğra", sertifika sahiplerinin imza oluşturma verilerini arşivlemez.

6.2.6. İmza Oluşturma Verisinin Kriptografik Modül Transferi

"e-tuğra", "ESHS" kök sertifikalarının imza oluşturma ve doğrulama verilerini, "e-tuğra"ya ait olan güvenli elektronik imza oluşturma aracı içerisinde (kriptografik modül) oluşturur.

"e-tuğra" imza oluşturma verisi yedekleme amacı ile güvenli modüllere transferi dışında kesinlikle "e-tuğra" güvenli elektronik imza oluşturma aracından çıkarılamaz. Yedekleme amacıyla imza oluşturma verisinin başka bir kriptografik modüle transferi gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili "güvenli personel" tarafından gerçekleştirilebilir.

"NES" sahiplerine ait imza oluşturma verileri güvenli elektronik imza oluşturma araçlarında oluşturulur ve oluşturuldukları güvenli elektronik imza oluşturma aracı dışarısına kesinlikle çıkarılamaz.

Anahtar üretiminin sertifika sahibi tarafında olduğundan, imza oluşturma verisinin kontrolü ve olası transferi sırasında güvenliğinin sağlanması sertifika sahibinin sorumluluğundadır.

6.2.7. Kriptografik Modülünde İmza Oluşturma Verisi Saklanması

"e-tuğra", kök sertifikalarının imza oluşturma ve doğrulama verileri üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma aracı içerisinde (kriptografik modül) saklanır.

"NES" sahiplerine ait imza oluşturma verileri üretildikleri ve Tebliğ'de tanımlı güvenlik düzeyine sahip güvenli elektronik imza oluşturma araçlarında saklanır. İmza oluşturma verisinin güvenli elektronik imza oluşturma aracı dışarısına çıkarılması ve değişikliğe uğraması engellenmiştir.

6.2.8. İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu

"e-tuğra" kök sertifikaları imza oluşturma verilerinin aktivasyonu, gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili "güvenli personel" tarafından erişim verilerinin kullanılması ile gerçekleştirilebilir.

"NES" sahiplerine ait imza oluşturma verisinin aktivasyonu güvenli elektronik imza oluşturma aracına sadece sertifika sahiplerinin sorumluluğunda erişim verisinin girilmesiyle sağlanır.

Sertifika sahibi, erişim verisinin üçüncü kişilerce izinsiz kullanımını ve çalınmasını önlemek için her türlü gerekli tedbirleri almakla yükümlüdür.

6.2.9. İmza Oluşturma Verisinin Aktif Durumdan Çıkarılması Metodu

"e-tuğra" kök sertifikaları imza oluşturma verileri sadece kullanım sırasında aktif halde tutulur, kullanım tamamlandıktan sonra aktif durumdan çıkarılır.

"NES" sahiplerine ait imza oluşturma verisinin, güvenli elektronik imza oluşturma aracı sistemden çıkarıldığında veya güvenli elektronik imza oluşturma aracı sisteme bağlıyken belli bir süre kullanılmadığında, etkinliği ortadan kalkar.

6.2.10. İmza Oluşturma Verisinin Yok Edilmesi Metodu

"e-tuğra" kök sertifikaları imza oluşturma verileri ve yedekleri geçerlilik sürelerinin sona ermesinden itibaren veya güvenlik problemleri sebebiyle gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili "güvenli personel" tarafından ilgili prosedürlere uygun olarak yok edilir ve kayıt altına alınır.

"NES" sahiplerine ait olan imza oluşturma verilerinin yok edilmesi, güvenli elektronik imza oluşturma aracının teknik yeterliliklerine bağlıdır. "NES" imza oluşturma verileri, verilerin silinmesi ile veya donanımın imha edilmesiyle yok edilebilir.

6.2.11. Kriptografik Modül Operasyonel Limitleri

"e-tuğra" güvenli elektronik imza oluşturma araçları ve "NES" sahiplerine sağlanan güvenli elektronik imza oluşturma araçları "Tebliğ"de belirtilen standartlara uygun üretilir ve saklanır.

6.3. Anahtar Çifti Yönetiminin Diğer Konuları

6.3.1. İmza Doğrulama Verisi Saklanması

"e-tuğra" "ESHS" kök sertifikaları, son kullanıcı sertifikaları ve bunlara bağlı imza doğrulama verileri en az 20 yıl boyunca saklanır. Saklama süresince verilerin bütünlüğünün sağlanması için gereken her türlü önlem alınır.

6.3.2. Sertifikanın Operasyonel Periyodu ve Anahtar Çifti Kullanımı Periyodu

Sertifikaların geçerlilik süresi, sertifikaların süresi dolduğunda veya iptal edildiğinde sona erer. İmza oluşturma ve doğrulama verilerinin geçerlilik süresi, ilgili sertifikaların geçerlilik süreleri ile aynıdır, ancak imza doğrulama verileri imza doğrulamak için kullanılmaya devam edilebilir. "e-tuğra" sertifikaların geçerlilik süresi başvuru sahibi, kurumsal başvuru sahibi ve/veya yetkilisi tarafından sertifika başvuru sırasında belirlenir.

"e-tuğra" "ESHS" kök sertifikalarının imza oluşturma verilerinin sertifika imzalama işlevine, sertifikanın geçerlilik süresi dolmadan önce uygun bir tarihte son verilir.

"e-tuğra" "NES" üretimi için kullanılan kök ve alt kök sertifikalarının geçerlilik süreleri en fazla on yıldır.

"NES" sertifikaları geçerlilik süreleri 1 (bir) yıl, 2 (iki) yıl ve 3 (üç) yıl olarak üretilir. Bu sertifikaların geçerlilik süreleri 39 (otuz dokuz) ayı geçemez.

6.4. Erişim Verileri

Erişim verileri, "güvenli personel"in teknik güvenlik gerektiren işlemlerde kullandığı şifreler ve erişim verileri, kök ve alt kök sertifikaların gizli anahtarlarının bulunduğu kriptografik modüllere ve anahtarların kullanılmasıyla ilgili erişim şifrelerine ve "NES" sahiplerinin güvenli elektronik imza oluşturma araçlarına erişim için kullandıkları şifrelerdir.

6.4.1. Erişim Verilerinin Oluşturulması ve Kurulumu

"e-tuğra" alt kök ve kök sertifikalarının anahtarların üretimini ve erişim şifrelerinin oluşturulması, ilgili e-tuğra prosedüründeki seremoni ile oluşturur. Kök ve alt kök sertifikaların gizli anahtarlarının kullanılması Bölüm 6.2.2'de açıklanmıştır.

"NES" sahipleri için erişim verileri "e-tuğra" tarafından yaratılır ve sadece sertifika sahiplerine teslim edilir. Ayrıca "e-tuğra" web sitesi üzerinden güvenli bir şekilde kendileri de aktivasyon işlemi ile oluşturabilirler.

Erişim verileri sahipleri kendi kontrolleri ile istedikleri zaman erişim verilerinde değişiklik yapabilirler.

6.4.2. Erişim Verilerinin Korunması

Erişim verilerinin "NES" sahiplerine ve "güvenli personel"e iletilmesinden sonra, verilerin gizliliğinin ve güvenliğinin korunması ile ilgili sorumluluk "NES" sahiplerine ve "güvenli personel"e aittir.

"e-tuğra" kök ve alt kök sertifikalarına ait gizli anahtarlar prosedürlerde belirtilen şekilde saklanır.

"e-tuğra" tüm sertifika sahiplerini erişim şifrelerini için, en az 6 (altı) karakter kullanılması, bir karakterin ardışık olarak tekrar etmemesi, doğum günü, isim ve benzeri tahmin edilmesini kolaylaştıran metotların kullanılmaması için uyarır. Tüm sertifika sahiplerine en fazla 6 (altı) ayda bir erişim şifrelerini değiştirmelerini ve farklı yeni bir şifre belirlemeleri telkin edilir.

6.4.3. Erişim Verileriyle İlgili Diğer Durumlar

"NES" sahiplerine verilen erişim verileri "KB"ler aracılığı ile kimlik tespiti yapılarak, güvenli kargoya (imza karşılığında kapalı zarf içerisinde) verilir veya "e-tuğra" web sayfası aracılığıyla ve gerekli kimlik kontrolü prosedürlerinin tamamlanmasıyla oluşturulur.

"e-tuğra" erişim şifrelerinin taşınması sadece "NES" sahipleri için geçerlidir. Güvenli kargo kullanılması durumunda, sertifikanın bulunduğu kart ile şifre zarfı farklı kurye şirketleri ile gönderilerek diğer kişilerin aynı anda eline geçmesi konusunda tedbir alınır.

Aktivasyon yönteminde erişim şifresi işlem anında sertifika sahibi tarafından belirlenir. Güvenlik adımları ve kontrolleri için “e-tuğra” sistemleri ile olan iletişim şifreli olarak gerçekleştirilir. Kullanılan aktivasyon kodu tek kullanımlıktır.

6.5. Bilgisayar Güvenlik Kontrolleri

6.5.1. Bilgisayar Güvenliği Teknik Gereklilikleri

“e-tuğra”da “ESHS” işleyişi içerisinde yürütülen operasyonlarda tüm iş ve işlemler bilgi güvenliği gereksinimleri doğrultusunda gerçekleştirilmektedir. “e-tuğra” bilgi güvenliği gereksinimleri, güvenli ve lisanslı yazılım ve donanımların kullanılması, ağ içerisinde saldırı tespit sistemlerinin bulunması, bilgi ve zilyetlik bazlı tanımlama yöntemleri ile erişim ve işlem kontrolü, “güvenli personel” arasında münhasır yetki ve görev dağılımı, gerekli tüm işlemlerin ve kayıtların yedeklenmesi ve saklanması yöntemleri ile sağlanır.

6.5.2. Bilgisayar Güvenliği Operasyonel Limitleri

İlgili değildir.

6.6. Yaşam Zinciri Teknik Kontrolleri

6.6.1. Sistem Geliştirme Kontrolleri

“e-tuğra” sertifika yaşam zinciri sistem geliştirme kontrolleri “e-tuğra” kalite yönetimi prosedürleri ve TS ISO/IEC 27001 denetimleri sonucunda ortaya çıkan risk azaltma metotları uyarınca gerçekleştirilir.

"e-tuğra", CA sistemlerinin edinilmesini ve geliştirilmesini kontrol etmek ve izlemek için mekanizmalara sahiptir. "e-tuğra", yazılımı yalnızca CA'nın çalışmasının bir parçası ise, yazılımı CA sistemlerine yükler. CA donanımları ve yazılımları, Sadece CA'nın işlemlerini gerçekleştirmeye adanmıştır.

6.6.2. Güvenlik Yönetim Kontrolleri

“e-tuğra” sertifika yaşam zinciri operasyonlarının güvenlik yönetimi kontrollerinin sağlanması için rutin olarak iç denetim prosedürlerini yürütür; ayrıca TS ISO/IEC 27001 uyumluluk denetimleri uyarınca yılda bir kere güvenlik yönetim kontrolleri açısından bağımsız denetçinin denetimine tabidir.

"e-tuğra", CA sistemlerinin güvenlikle ilgili yapılandırmalarını kontrol etmek ve izlemek için mekanizmalara sahiptir. Tüm sistem kontrolleri ve izlemeleri, yıllık, üç aylık veya aylık zaman planlarında önceden geliştirilmiş prosedür ve talimatlara göre yapılır.

6.6.3. Yaşam Zinciri Güvenlik Kontrolleri

İlgili değildir.

6.7. Ağ Güvenlik Kontrolleri

“e-tuğra” “Güven Merkezi”nin anahtar üretimi, sertifika yaşam döngüsü kontrolleri ve diğer sistemleri gerekli ağ güvenliği alt yapısına sahiptir. Ağ güvenliğinin sağlanmasında güvenlik duvarları, yönlendiriciler, anahtarlama cihazları gibi donanımlar gerekli konfigürasyonda yapılandırılmıştır. “e-tuğra” ağ güvenliği yönetimi “Ağ Yönetim Prosedürleri” uyarınca gerçekleştirilir. “KB”ler “e-tuğra” “Güven Merkezi”ne elektronik ortamda bilgi iletmeleri halinde, ağ güvenliği sağlanmış internet bağlantısı kullanırlar.

İlgili prosedürler uyarınca, ağ elemanları sürekli izlenmekte, iç veya dış noktalardan gelebilecek saldırılar ve yetkisiz erişimler tespit edilmekte ve diğer güvenlik kontrolleri aracılığıyla da saldırılar engellenmektedir. Ayrıca düzenli olarak yapılan zayıflık ve penetrasyon testleri sonucu bulunan zayıflıkların ve açıklıkların belli planlar çerçevesinde giderilmesi de sağlanmaktadır.

“e-tuğra” ağına dışarıdan yapılabilecek her türlü erişim şifrelenmiş kanallar üzerinden sağlanmakta ve sadece sunulan hizmetlere erişime izin verilmektedir. Hassas bilgilerin bulunduğu sistemlere erişim ise sadece “e-tuğra” güven merkezindeki yetkili ağlar üzerinden yapılabilmektedir.

“e-tuğra” ağ güvenliği ile ilgili işlemlerini ETSI EN 319 411-1 ve ISO 27001 dokümanlarının gereksinimlerini yerine getirerek yürütür. Bu gereksinimler genel olarak aşağıdaki şekilde sıralanabilir;

6.8. Zaman Damgası

“e-tuğra” sertifika yaşam döngüsünün sağlanması sırasında ilgili işlemlerde oluşan elektronik kayıtların zaman bilgisi, zaman damgası hizmetlerinde kullanılan zaman kaynağı ile eş güdümlüdür. Kayıt bütünlüğü anahtarlanmış özet yöntemi kullanılarak korunur ve arşivleme aşamasında zaman damgası kullanılır.

7. SERTİFİKA, SERTİFİKA İPTAL LİSTESİ (“SİL”) VE “ÇSDP” PROFİLLERİ

7.1. Sertifika Profili

“e-tuğra” sertifikaları; “ISO/IEC 9594-8/ ITU-T Recommendation X.509: “Information Technology- Open Systems Interconnection- The Directory: Public –key and attribute certificate frameworks” ile “IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” dokümanlarına uygun olarak hazırlar.

“e-tuğra” Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan “Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007” dokümanına uygunluk sağlanır.

“Sertifikayı Veren” (Issuer) olarak, “e-tuğra”, “O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.” unvanıyla yazılır.

7.1.1. Sürüm Numaraları

“e-tuğra”ya ait kök ve alt kök sertifikaları ile son kullanıcı sertifikaları, “IETF RFC 5280” adlı dokümanda belirtilen X.509 v3’e uygundur.

7.1.2. Sertifika Uzantıları

“e-tuğra” kök sertifikalarında ve “NES”lerde X.509V.3 (2000) ve ETSI TS 101 862’de desteklenen bütün uzantılar kullanılabilir.

“NES”ler, “IETF RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile” ve “Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007” dokümanları uyarınca tanımlanan nitelikli elektronik sertifika uzantılarını içerir.

“e-tuğra” sertifikalarında temel olarak aşağıdaki alanları içerir.

- **Seri No:** Eşsiz numara (Sertifikayı veren için)
- **Geçerlilik Başlangıcı**: RFC 5280'e göre kodlanmış UTC zamanı
- **Geçerlilik Sonu:** RFC 5280'e göre kodlanmış UTC zamanı
- **Açık Anahtar:** RFC 5280'e göre kodlanmış anahtar değeri
- **İmza**: RFC 5280'e göre kodlanmış imza değeri.

Tüm sertifika tiplerinde, sertifika içerisinde aşağıdaki sertifika uzantıları standart olarak bulunur:

- **Authority Key Identifier (Yetkili Anahtarı Tanımlayıcısı):** Sertifikayı yayımlayan “e-tuğra” sertifikasının açık anahtar özet değeri.
- **Subject Key Identifer (Özne Anahtarı Tanımlayıcısı):** Sertifikada yer alan açık anahtarın özet değeri.
- **Basic Constraints (Temel Kısıtlar):** CA değeri “false” olarak işaretlenir.
- **CRL Distribution Points (SİL Dağıtım Noktaları):** Sertifikayı yayımlayan “e-tuğra” sertifikası tarafından imzalanmış olan “SİL” (CRL) dosyasının URL adresi.
- **Authority Information Access (ESHS Bilgi Erişimi)**: Sertifikayı yayımlayan “e-tuğra” sertifikasına ve “ÇSDP” servisine erişim adresleri.

“NES” Uzantıları

“e-tuğra” tarafından üretilen “NES”lerde standart uzantılara ek aşağıdaki uzantılar bulunur:

Key Usage (Anahtar Kullanımı): Digital signature (elektronik imza) ve nonrepudiation (inkar edilemezlik) değerleri bulunur. Uzantı kritik olarak işaretlenir.

Certificate Policies (Sertifika İlkeleri):

- İlke Tanımlayıcı Numarası (Policy Identifier) olarak 2.16.792.3.0.4.1.1.1 (“e-tuğra” “NES” OID) değeri,
- Sertifika Uygulama Esasları adresi (Policy Qualifier Info – CPS) olarak http://www.e-tugra.com.tr/cps değeri,
- “Kullanıcı Uyarısı (Policy Qualifier Info – User Notice) olarak “Bu sertifika 5070 sayılı Elektronik İmza Kanunu’na göre nitelikli elektronik sertifikadır.” ibaresi kullanılır.

Subject Alternative Name (Özne Alternatif Adı): (Opsiyonel) Sertifika sahibinin elektronik posta adresi kullanılır.

Qualified Certificate Statements (Nitelikli Sertifika İbareleri):

- ETSI TS 101 862 uyumunu belirten nesne tanımlayıcısı (0.4.0.1862.1.1),
- Bilgi Teknolojileri ve İletişim Kurumu uyumunu belirten nesne tanımlayıcısı (2.16.792.1.61.0.1.5070.1.1),
- Opsiyonel olarak Para Limiti İbaresi kullanılmaktadır.

7.1.3. Algoritma Nesne Tanımlayıcıları

“e-tuğra” tüm sertifikaların imzalanmasında tabi olduğu “tebliğ” uygun olmak koşulu ile aşağıdaki algoritmalardan birini kullanılır ve nesne belirteçleri sertifika içerisinde belirtilir.

- “SHA-256 with RSA” (1.2.840.113549.1.1.11),
- “SHA-384 with RSA” (1.2.840.113549.1.1.12),
- “SHA-512 with RSA” (1.2.840.113549.1.1.13)

Tüm son kullanıcı sertifikalarının tamamı SHA- 256 algoritmasıyla üretilmektedir. Bu sertifikaların üretiminde kullanılan kök sertifikalar halen SHA-1 veya SHA- 256 olmakla birlikte, yeni üretilen tüm kök ve alt kök sertifikalarda SHA – 256 ile gerçekleştirilmektedir.

7.1.4. İsim Formları

Sertifikalardaki isim alanlarında ITU X.500 “Distinguished Name” (Tekil Kayıt Adı) biçimine uygun isimler kullanılır.

“Sertifikayı Veren” (Issuer) olarak, “e-tuğra” “O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.” unvanıyla yazılır.

7.1.5. İsim Kısıtlamaları

Sertifikalarda anonim veya takma adlar kullanılamaz. adların tekliğini sağlamak için T.C. kimlik numarası, yabancı kişiler için ülke kodu ve pasaport numarası kullanılır.

7.1.6. Sertifika İlkeleri Nesne Belirteci

Sertifikaların “sertifika ilkeleri” uzantısında, sertifikanın tipine göre 1.2 bölümünde belirtilen sertifika ilkeleri nesne belirteci numarası (OID) kullanılır.

7.1.7. Sertifika İlkeleri Kısıtlamaları Uzantısının Kullanımı

Alt kök sertifikalarında amacına göre ihtiyaç duyulmasında ilke kısıtları uzantısı kullanabilir.

7.1.8. Sertifika İlkeleri Belirteçleri için Yazımsal ve Anlamsal Özellikler

Sertifikaların sertifika ilkeleri uzantısında "SUE"ye erişimi sağlayan bir URL bulunur.

"e-tuğra" tarafından yayınlanan bir nitelikli elektronik sertifika olduğuna dair bir ibare QcStatements-Statement ID altında "Bu sertifika 5070 sayılı Elektronik İmza Kanunu'na göre nitelikli elektronik sertifikadır" şeklinde yer alır. Ayrıca aynı bölümde nitelikli sertifikaya ait "2.16.792.1.61.0.1.5070.1.1" nesne belirteci bulunur.

7.1.9. Kritik Sertifika İlkeleri Uzantısının İşlenme Semantiği

Koşul yoktur.

7.2. "SİL" Profili

"e-tuğra" RFC 3280'a uygun "SİL"ler düzenler. "SİL"lerde "e-tuğra" "ESHS" sertifikası ile atılmış elektronik imza, "SİL"in yayınlanma tarihi, bir sonraki "SİL"in yayınlanma tarihi, iptal edilen sertifikaların seri numaraları ve iptal edilme zamanı yer alır. "SİL"ler, Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007"ye uygun hazırlanır.

7.2.1. Sürüm Numarası/Numaraları

"SİL"ler ITU X.509 V.2 "SİL" formatına uygun olarak hazırlanır.

7.2.2. "SİL" ve "SİL" Girdi Uzantıları

"e-tuğra" tarafından yayınlanan "SİL"lerde RFC 3280 tarafından tanımlanan uzantılar kullanılır.

7.3. Çevrimiçi Sertifika Durum Protokolü ("ÇSDP") Profili

"ÇSDP" gerçek zamanlı sertifika sorgusu hizmetidir. ÇSDP cevap mesajları, Bilgi Teknolojileri ve Telekomünikasyon Kurumu tarafından yayımlanan "Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri – Nisan 2007"ye uygun hazırlanır.

7.3.1. Sürüm Numarası (Veya Numaraları)

RFC 2560 desteklenmektedir.

7.3.2. "ÇSDP" Uzantıları

RFC 2560 desteklenmektedir.

8. UYUM DENETİMİ VE DİĞER DEĞERLENDİRMELER

“e-tuğra” sunmuş olduğu “ESHS” hizmetleri ve yürütmüş olduğu “ESHS” operasyonları bakımından Elektronik İmza’ya ilişkin emredici mevzuat hükümleri gereğince Bilgi Teknolojileri ve İletişim Kurumu’nun denetimine tabidir. Ayrıca Bilgi Teknolojileri ve İletişim Kurumu en az iki yılda bir kere olmak üzere “e-tuğra”nın mevzuata ve standartlara uygun olarak işleyişini sürdürmesini denetler.

“e-tuğra” “ESHS” süreçlerinde ETSI EN 319 411-1 standardı ve TS ISO/IEC 27001 sertifikası gereğince bilgi güvenliği açısından periyodik denetimlere tabi tutulur. Ayrıca, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemine göre risk değerlendirmelerini gerçekleştirir. Bunun sonucunda, iş riskleri değerlendirilir ve gerekli güvenlik koşulları ve işletim prosedürleri belirlenir. Risk analizi düzenli olarak gözden geçirilir ve gerektiğinde güncelleme yapılır.

“e-tuğra” ETSI EN 319 411-1 standardı kapsamında da yetkili bir denetçi kurum tarafından “e-tuğra”nın bu doküman kapsamı dışında olan SSL ve KIS süreçleri denetime tabi tutulur.

“e-tuğra”, yukarıda sayılan uygunluk denetimlerinin yanı sıra kendi personeli tarafından gerçekleştirilen iç denetim süreçlerini devamlı olarak yerine getirir.

8.1. Denetim Sıklığı ve Denetim Durumları

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlerin sıklığı, Kurum yetkililerinin inisiyatifinde olmakla beraber, en az iki yılda bir yapılacaktır. Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem denetleme istemleri yerine getirilir.

TS ISO/IEC 27001 sertifikasına bağlı uyumluluk denetimleri her yıl yapılır.

ETSI EN 319 411-1 denetim standardı kapsamında “e-tuğra”nın bu doküman kapsamı dışında olan SSL ve KIS hizmet süreçleri her yıl uygunluk denetimine tabi tutulur.

“e-tuğra” iç denetimleri yetkili “e-tuğra” personeli tarafından belirlenen periyodların dışında gerekli görülen durumlarda da yapılır.

8.2. Denetleme Yapan Kişinin Tanımlanması ve Nitelikleri

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimler yetkili Kurum peroneli tarafından yapılır.

TS ISO/IEC 27001 sertifikasına bağlı uyumluluk denetimleri yetkili bir denetçi tarafından yapılacaktır.

ETSI 102 042 denetimi gerçekleştirecek denetçi; Açık Anahtarlı Altyapı (“AAA”) teknolojisi, bilgi güvenliği sistemleri ve teknikleri, bilgi teknolojileri ve güvenliği denetimi ve üçüncü parti bağımsız raporlamaları konularında yetkinliğine sahip olmalıdır. Ayrıca European Cooperation for Accreditation gibi resmi bir akreditasyon kuruluşu tarafından ISO/IEC 17021’e uyumlu olduğuna dair ve CEN Workshop Agreement (CWA) 14172-2 standardının 3.4 maddesi uyarınca da akredite edilmiş olmalıdır.

“e-tuğra” iç denetimleri yetkili “e-tuğra” “güvenli personel” tarafından yapılacaktır.

8.3. Denetim Yapan Kişinin "ESHS" ile İlişkisi

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlere ilişkin usul ve esaslar Kurum tarafından belirlenir.

TS ISO/IEC 27001 sertifikası bağımsız bir denetçi tarafından yapılacaktır.

ETSI EN 319 411-1 denetimi, bağımsız ve yetkili bir denetçi tarafından yapılacaktır.

“e-tuğra” iç denetimleri yetkili “e-tuğra” “güvenli personel”i tarafından yapılacaktır.

8.4. Denetimde Kapsanan Konular

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlerde “e-tuğra”nın elektronik imzayla ilgili mevzuat uyarınca üstlenmiş olduğu yükümlülüklerini yerine getirip getirmediği denetlenir.

TS ISO/IEC 27001 sertifikasına ilişkin denetimlerde “e-tuğra” “Güven Merkezi” operasyonları ve “ESHS” işleyişine ilişkin süreçler denetlenir.

ETSI EN 319 411-1 denetimi “e-tuğra”nın bu doküman kapsamı dışında diğer sertifika türlerinde verdiği hizmetlerine ilişkin tüm süreçleri, bu hizmetler için kullanılan teknik altyapı ve hizmetlerin verildiği tesisleri içermektedir.

“e-tuğra” iç denetimleri ISO/IEC 27001 ve ETSI EN 319 411-1 standartlarının kontrol maddelerine ilişkin tüm hükümleri kapsamaktadır.

8.5. Eksikliğin Ortaya Çıkması Durumunda Gerçekleştirilecek Eylemler

“e-tuğra” tarafından gerçekleştirilen iç denetimlerde herhangi bir eksikliğin tespit edilmesi halinde eksiklik yetkili “e-tuğra” personeli tarafından mümkün olan en kısa sürede düzeltici ve önleyici faaliyet düzenlenerek giderilir.

TS ISO/IEC 27001 denetimleri sırasında saptanan minör nitelikteki eksiklikler bir sonraki denetim dönemine kadar “e-tuğra” tarafından giderilir; eksiklerin majör nitelikte olması halinde sertifika geri alınır.

ETSI EN 319 411-1 standardına uyumu kapsamında gerçekleştirilen denetimler sırasında saptanan minör nitelikteki eksiklikler bir sonraki denetim dönemine kadar “e-tuğra” tarafından giderilir; eksiklerin majör nitelikte olması halinde eksikliğin niteliğine göre sertifika geri alınabilir.

Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimlerde “e-tuğra”nın mevzuattan ve ilgili standartlardan doğan yükümlülüklerini yerine getirmemesi durumunda mevzuatta öngörülen yaptırım ve cezalar “e-tuğra”ya karşı uygulanır.

8.6. Denetim Sonuçlarının Yayınlanması ve İlgili Taraflara İletimi

Kanun gereği Bilgi Teknolojileri ve İletişim Kurumu tarafından yapılan denetimin sonuçları gerek duyulduğu takdirde resmi yollarla “e-tuğra” iletilir. Kurum’un bir geri bildirimde bulunmaması, olumsuz bir değerlendirmenin olmadığı anlamını taşır.

TS ISO/IEC 27001 denetimlerinin sonuçları, denetçi firma tarafından “e-tuğra”ya iletilir. ETSI EN 319 411-1 denetimlerinin sonuçları, denetçi firma tarafından “e-tuğra”ya iletilir.

“e-tuğra” tarafından yapılan iç denetimlerin sonuçları “e-tuğra” yönetimine ve ilgili “güvenli personel”e iletilir. İç denetim sonuçları ise, iç denetim sonuç raporlarında yer alır ve ilgili yetkililerin değerlendirmesine sunulur.

9. DİĞER TİCARİ VE HUKUKİ KONULAR

9.1. Ücretler

9.1.1. Sertifika Oluşturma veya Yenileme Ücretleri

"e-tuğra" tarafından üretilen sertifikalar, çeşitlerine, geçerlilik sürelerine göre ve içeriklerinde yer alan maddi işlem sınırı ölçüsünde, sertifika üretim maliyetleri ve piyasa koşulları uyarınca fiyatlandırılır. Maddi işlem sınırı, sertifika mali sorumluluk sigortası primleri sertifika fiyatlarına yansıtılır. Güncel sertifika ücretleri, "e-tuğra" web sitesi ve uygun görülen diğer iletişim kanalları üzerinden yayınlanır.

Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 13. maddesine göre; "e-tuğra"nın imza oluşturma verisinin çalınması, kaybolması, gizliliğinin veya güvenilirliğinin ortadan kalkması ya da sertifika ilkelerinin değişmesi gibi sertifika sahibinin kusurunun bulunmadığı durumların sonucunda nitelikli elektronik sertifikaların "e-tuğra" tarafından iptal edilmesi ve yenilenmesi halinde, yenileme işlemleri için ücret talep edilemez.

9.1.2. Sertifikalara Erişim Ücretleri

"e-tuğra" sertifika sahipleri tarafından herkesin erişimine açılan sertifikalar için erişim hizmetlerine yönelik ücret talep etmez.

9.1.3. Sertifikaların İptal veya Durum Kayıtlarına İlişkin Bilgilere Erişim Ücretleri

"e-tuğra" ürettiği sertifikalara ilişkin iptal ve durum bilgileri "SİL"ler ve "ÇSDP" aracılığıyla ilgililere duyurulur. "e-tuğra" "SİL"ler ve "ÇSDP"ne erişim için herhangi bir ücret talep etmez.

9.1.4. Diğer Hizmetlerin Ücretleri

"e-tuğra", Kanun ve uygulamalar gereği, kamuya açık olarak yayınladığı "Sİ", "SUE", sertifika sahibi ve sertifika hizmetleri taahhütnameleri gibi kitapçık ve belgeler için ücret talep etmez. Bunların dışında kalan ve katma değerli olarak üretilerek müşterilere sunulan diğer ürün ve hizmetler için uygulanacak ücretler, web sitesi ve diğer iletişim kanalları üzerinden müşterilere duyurulur.

"e-tuğra" dokümanlarının; çoğaltma, başkalarına dağıtma, değişiklik veya işleme gibi inceleme veya sertifikalar ile ilgili süreçlerde kullanma haricindeki amaçlarla kullanımına izin vermez.

9.1.5. Geri Ödeme Politikası

"e-tuğra", Sertifika hizmetlerinde bedel iadesi yapmaz.

Sadece, "e-tuğra"dan kaynaklanan nedenlerle, sertifika içeriğinin başvurudan farklı verilerin bulunması durumunda, herhangi bir ücret talep edilmeden sertifikası iptal edilir ve yeni bir başvuru ile yeni bir sertifika verilir.

İptal edilen sertifikaların iptal edildiği andan geçerlilik süresinin sonuna kadar olan kısmının ücreti mahsup veya geri iade edilmez.

"e-tuğra"dan kaynaklanan nedenlerle reddedilen sertifika başvuruları ücretleri, talep edilmesi durumunda ücret iade edilir.

9.2. Finansal Sorumluluk

“e-tuğra” Elektronik İmza Kanunu’nun 13.maddesine göre “NES”ler için zorunlu sertifika mali sorumluluk sigortası yaptırmak zorundadırlar. “Sertifika Mali Sorumluluk Sigortası Yönetmeliği” Madde 6 uyarınca, zorunlu sertifika mali sorumluluk sigortası, "ESHS"nin güvenli ürün ve sistemlerini kullanma, hizmeti güvenilir bir biçimde yürütme ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini yerine getirmemesi dolayısıyla zarar görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar.

9.2.1. Sigorta Kapsamı

“NES”ler için, zorunlu sertifika mali sorumluluk sigortası:

- “ESHS”nin güvenli ürün ve sistemlerini kullanma, hizmeti güvenilir bir biçimde yürütme, sertifikaların taklit ve tahrif edilmesini önleme ile ilgili görevlerini gerektiği biçimde yerine getirmemesi,
- Sertifikaların içeriğinde “ESHS”den kaynaklanan yanlış bilgilerin bulunması,
- Sertifikaların oluşturulması sırasında nitelikli elektronik imza sahiplerinin verdikleri bilgilerin “ESHS” tarafından eksik veya yanlış işlenmesi sonucu ortaya çıkan hataların bulunması,
- Sertifikaların “ESHS” ile “NES” sahipleri arasında yapılan sözleşmeye tam ve uygun olarak hazırlanmaması,

gibi “ESHS”nin ve eylemlerinden sorumlu bulunduğu personelin kusurundan, ihmalinden veya gerekli özeni göstermemesinden doğan maddi zararları kapsar.

Aşağıdaki hallerden birinin veya birkaçının sonucunda doğan sorumluluğa bağlı olarak;

- Savaş, düşman hareketleri, çarpışma (savaş ilan edilmiş olsun veya olmasın), ihtilal, ayaklanma ve bunların gerektirdiği inzibati askeri hareketlerden,
- Herhangi bir nükleer yakıttan veya nükleer yakıtın yanması sonucu nükleer atıklardan veya bunlara atfedilen sebeplerden meydana gelen iyonlayıcı radyasyonlar veya radyo-aktivite bulaşmaları ve bunların gerektirdiği inzibati ve askeri tedbirlerden,
- Deprem, yanardağ püskürmesi, deniz depremi, sel, seylap ve su baskını, yer kayması gibi doğal afetlerden,
- Kamu otoritesi tarafından yapılacak tasarruflar sonucunda oluşan ve “ESHS”nin kusurundan kaynaklanmayan sorunlardan,
- İletişim altyapısı ve “ESHS”nin doğrudan kontrolü altında olmayan bilgi işlem altyapısında meydana gelen sorunlardan,
- İmza sahibi tarafından kanun dışı amaçlar için nitelikli elektronik imzanın kullanılmasından,
- Sigortacıya veya sigorta ettirene haber verildikten sonraki bir tarihte “ESHS” tarafından iptal edilmeyip ikinci veya daha çok miktarda hasar oluşmasına neden olan aynı nitelikli elektronik sertifika ile işlem yapılmasından,
- Faaliyet konusu ile ilgili kanun, yönetmelik ve tebliğlerle belirlenen esaslar ve teknik standartlara bağlı kalınmamasından,

doğan zararlar sigorta teminatı dışındadır.

9.2.2. Diğer Varlıklar

İlgili değildir.

9.2.3. Son Kullanıcılar İçin Sigorta veya Diğer Garantilerin Kapsamı

Bkz. Bölüm 9.2.1

9.3. Ticari Bilgilerin Gizliliği

9.3.1. Gizli Bilgilerin Konusu

"e-tuğra"nın teknik ve operasyonel anlamda işlemlerine ilişkin bilgi güvenliği kapsamında gizli sayılan tüm bilgi ve belgeler, iş planları, satış bilgileri, işbirliği sözleşmeleri, iş ortaklığı yapılan kuruluşlara ait gizlilik dereceli bilgiler gibi ticari faaliyetlerine ilişkin her türlü gizli bilgi ve belge, kök ve alt kök sertifikaları imza oluşturma verileri, işlem kayıtları, sertifika sahiplerinin "Kanun" kapsamında "kişisel veri" sayılan bilgileri, denetim ve değerlendirme kayıtları, "Güven Merkezi" ile ilgili her türlü gizli bilgi ve belge, donanım ve yazılımla ilgili teknik güvenlik bilgileri, tesis içi bölge ve cihazlara ait erişim şifreleri, tesis planı ve iç tasarımı gizli bilgi kapsamındadır.

9.3.2. Gizli Bilgilerin Konusu İçerisinde Olmayan Bilgiler

"SUE", "Sİ", kullanıcı sözleşmeleri gibi Kanun ve uygulamalar gereği kamuya açık olması gereken ve "e-tuğra" web sitesinde ve bilgi deposunda bulunan bilgiler, sertifika sahibinin rızası doğrultusunda kamuya açık bir dizinde "e-tuğra" tarafından yayınlanan sertifikalar, "e-tuğra" kök ve alt kök sertifikaları, "SİL"ler gizli bilgi kapsamında sayılmazlar.

9.3.3. Gizli Bilgilerin Korunmasına İlişkin Sorumluluklar

"e-tuğra" çalışanlarının tamamı gizli bilgilerin korunması konusunda sorumluluk sahibidir. Güvenlik politikaları gereği hiçbir gizli bilgiye, yetkilisi dışındaki çalışanların ya da üçüncü kişilerin erişimine izin verilmez. Bilgi güvenliğinin sağlanmasıyla ilgili tüm prosedürler çalışanlar tarafından eksiksiz uygulanır.

Elektronik İmza Kanunu'nun 12. maddesine göre "e-tuğra"; sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez, sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz.

9.4. Kişisel Bilgilerin Mahremiyeti (Gizliliği)

9.4.1. Mahremiyet Planı

"e-tuğra" verdiği hizmetler ve Kanun kapsamındaki yükümlülükleri doğrultusunda sertifika sahiplerinin ve diğer katılımcıların kişisel bilgilerini korur.

9.4.2. Özel Sayılan Bilgiler

Sertifika sahibinden sertifika başvurusu sırasında alınan ve sertifika içeriğinde ve "SİL"lerde yer almayan bilgiler özel bilgilerdir.

9.4.3. Özel Sayılmayan Bilgiler

Sertifika ve "SİL"lerde herkesin erişimine açık bir şekilde yayınlanan bilgiler özel sayılmayan bilgilerdir.

Sertifika sahibinin izin vermemesi durumunda "e-tuğra" ilgili sertifikayı kamuoyunun erişimine açmaz.

9.4.5. Özel Bilgiyi Kullanma Bildirimi ve Onayı

"e-tuğra", "SUE" ve "Sİ" dokümanı ile sertifika sahibi taahhütnamesin de belirtilmiş amaçlar için sertifikayı, sertifika başvurusunda sağlanmış bilgileri kullanabilir.

9.4.6. Adli ve İdari Süreçlerde Kullanılmak Üzere Yapılan Açıklamalar

"e-tuğra" sertifika sahipleri ve ilgili taraflar, "e-tuğra"nın, yürürlükteki emredici mevzuat hükümleri gereğince resmi makamlara açıklama yapmakla yükümlü olduğu durumlar içerisinde, resmi makamlarca yürürlükteki emredici mevzuat hükümlerine uygun bir şekilde talep edilmesi halinde gizli/özel bilgileri resmi makamlara açıklamaya yetkili olacağını kabul eder.

Bilgi Teknolojileri ve İletişim Kurumu'nun denetimleri sırasında "ESHS"ler "Kanun" uyarınca Kurum yetkililerine talep ettikleri her türlü bilgi ve belgeleri vermek zorundadırlar.

Sertifika sahipleri ve ilgili taraflar, "e-tuğra"nın, iyi niyet çerçevesinde, mahkeme celpleri, soruşturma evrakı, karşılıklı dilekçeler, delil ve doküman talepleri gibi hukuk veya idari davalarla ilgili keşif süreci sırasında adli, idari veya diğer yasal süreçlere cevaben gerekli olduğunu düşünmesi halinde gizli/özel bilgileri açıklamaya yetkili olacağını kabul eder.

9.4.7. Bilgilerin Açıklandığı Diğer Durumlar

İlgili değildir.

9.5. Fikri Mülkiyet Hakları

"e-tuğra" tarafından yayınlanan tüm sertifikalar ve kök sertifikalar, sertifika iptal bilgileri, "SUE", "Sİ", kullanıcı sözleşmeleri, bilgi deposunda yayınlanan ve "e-tuğra" tarafından oluşturulmuş her türlü doküman, "e-tuğra" tarafından oluşturulan her türlü veritabanı, "e-tuğra"ya ait web siteleri ve bu web sitelerinde yer alan her türlü metin, görsel ve işitsel içeriğin fikri mülkiyet hakları "e-tuğra"ya aittir.

Sertifika sahiplerinin ve kurumsal başvuru sahiplerinin, sertifika başvurusunda yer alan kendilerine ait herhangi bir ticari marka, hizmet markası, servis işareti veya ticari isim ve ünvanla ilgili sahip oldukları (varsa) bütün hakları saklıdır.

9.6. Sorumluluk ve Garantiler

9.6.1. "ESHS"nin Sorumluluk ve Garantileri

"e-tuğra"; ürettiği tüm sertifikaların içeriğinin doğru olduğunu, kimlik doğrulama işlemlerinin tam yapıldığına, sertifikanın sadece başvuru yetkisi olan başvuru sahibi adına üretildiğini ve doğru kişiye teslim edildiğini, sertifika durum bilgilerinin güncelliğini ve doğruluğunu; "Sİ" ve "SUE"de yer alan tüm uygulama gereklilikleri ve yükümlülüklerini yerine getireceğini garanti eder.

"e-tuğra"; "NES" verebilmek için, Kanun'un 10. Maddesi ve Yönetmeliğin 14. Maddesinde yer alan yükümlülükleri yerine getirir.

"e-tuğra" sunmuş oldukları elektronik sertifika, zaman damgası ve elektronik imzayla ilgili hizmetleri elektronik imzayla ilgili emredici mevzuat doğrultusunda yürütür. "ESHS", "Kanun" veya bu Kanuna

dayanılarak çıkarılan "Yönetmelik" hükümlerinin ihlâli suretiyle üçüncü kişilerin zararına sebebiyet verecek olursa bu zararı tazminle mükelleftir. "e-tuğra" sertifika sahiplerine ve üçüncü kişilere karşı sorumluluğunu ancak sertifikanın kullanım ve maddi kapsama ilişkin sınırlamaları anlamında kısıtlayabilir. "e-tuğra", sertifika içerisinde belirtilen maddi kapsama ve/veya kullanıma ilişkin sınırlamaların dışında kullanılması durumunda, bu sınırlama dışı kullanımlardan dolayı doğacak zararları tazminle mükellef değildir. "e-tuğra", "Kanun" ve ilgili mevzuattan doğan yükümlülüklerini yerine getirmemesi sonucu ortaya çıkacak zararların karşılanması amacıyla Kanun'un 13.maddesinde belirtilen zorunlu sertifika malî sorumluluk sigortasını yaptırır.

9.6.2. Kayıt Birimi Sorumlulukları

"KB"ler, sertifika başvurularının alınmasından, sertifika başvuru sahibinin sertifika tipine göre ilgili "SUE" dokümanın da belirtilen kimlik bilgilerinin gerekli belgelere dayanarak tespitinden, sertifika sahibinden gerekli belgeleri ve bilgileri alarak "e-tuğra"ya iletmekten, sertifika yenileme, askı ve iptal taleplerini kabul ederek "e-tuğra"ya iletmekten sorumludur.

"NES" için anahtar çifti üretme yetkisi olan "KB"ler, üretimin güvenliğinden sorumludur.

"e-tuğra", sertifikalarda bulunan bilgilerin doğruluğundan sertifika sahiplerine ve üçüncü kişilere karşı münhasıran sorumludur. "e-tuğra"nın kendi organizasyonu içerisinde doğrudan yer almayan "KB"ler ile "e-tuğra" arasındaki sorumluluk rejimi "Kayıt Birimi Hizmet Sözleşmesi" uyarınca belirlenir.

9.6.3. Sertifika Sahibi ve Kurumsal Başvuru Sahibinin Sorumlulukları

Sertifika sahipleri, sertifika başvurusu, yenileme ve iptal talepleri sırasında "e-tuğra"ya doğru bilgi ve belgeler sunmak, sertifikalarını "Sİ" ve "SUE" dökümanların da yer alan koşullar uyarınca kullanmak, sertifika kullanıcı sözleşmesinde/taahhütnamesinde yer alan tüm yükümlülüklerini yerine getirmekle yükümlüdür.

Sertifika sahibi, kullanımdan önce sertifikanın geçerlilik durumunu kontrol etmekle, geçerliliği sona ermiş, askıda bulunan veya iptal edilmiş sertifikayı kullanmamakla yükümlüdür.

Sertifika sahipleri ise, sertifikayı sadece güvenli elektronik imza oluşturma ve doğrulama süreçlerinde kullanmakla, kendilerine ait olan imza oluşturma verisini kimseye kullandırmamakla, erişim verisinin gizliliğini sağlamakla, sertifikayı kullanım ve maddi kapsama ilişkin sınırlar dahilinde kullanmakla, sertifikanın kullanıldığı ortamların gizliliğini ve güvenliğini sağlamakla, imzalamış olduğu kullanıcı sözleşmesine, "SUE"ye, "Sİ"ye uygun olarak ve hukuka uygun amaçlarla kullanmakla yükümlüdür. Sertifika sahiplerinin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğan veya doğmuş olacak "e-tuğra"nın, üçüncü kişilerin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır.

Kurumsal başvuru sahibi, adlarına "NES" başvurusunda bulunduğu "NES" sahiplerinin kimlik bilgilerini "e-tuğra" tarafından belirlenen belgeler doğrultusunda tespit etmeye, "NES" başvuru sahiplerinin "NES" sahibi olmak konusundaki yazılı rızalarını almaya ve "e-tuğra" tarafından belirlenen bilgi ve belgeleri "NES" başvuru sahiplerinden temin ederek "e-tuğra"ya iletmekle yükümlüdür.

Kurumsal başvuru sahibi, adına "NES" başvurusunda bulunduğu kimselerin tespit ettiği kimlik bilgilerinin "Sİ", "SUE" ve "e- tuğra" web sitesinde belirtilen resmi belgelere dayanmasından ve doğru olmasından sorumludur. Kurumsal başvuru sahiplerinin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğmuş ve doğacak olan "e-tuğra"nın, üçüncü kişilerin, "NES" sahiplerinin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır.

9.6.4. Üçüncü Kişilerin Sorumlulukları ve Garantileri

Üçüncü kişiler "NES" ile ilişkili olarak oluşturulmuş bir güvenli elektronik imzaya güvenerek herhangi bir iş veya işlem yapmadan önce güvenli elektronik imzayı doğrulamakla ve "NES"in geçerliliğini kontrol etmekle yükümlüdürler. Üçüncü taraflar bu sorumluluklarını "güvenli elektronik imza doğrulama aracı" kullanarak yerine getirebilirler. Üçüncü kişiler aynı zamanda "Yönetmelik"in 16. Maddesinde belirtilen yükümlülüklere uymakla mükelleflerdir.

Üçüncü kişilerin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğmuş ve doğacak "e-tuğra"nın, sertifika sahiplerinin, kurumsal başvuru sahiplerinin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır.

9.6.5. Diğer Katılımcıların Sorumlulukları ve Garantileri

"e-tuğra" "ESHS" işleyişini sürdürürken üçüncü taraflarla bazı hizmetlerin görülmesi için hizmet sözleşmeleri yapabilir. Bu üçüncü tarafların sorumlulukları kendileriyle yapılan hizmet sözleşmeleri uyarınca belirlenir. Hizmet sözleşmesi üçüncü kişilerin, "e-tuğra" iş süreçleri ve "e-tuğra" müşterileriyle ilgili gizli veya özel bilgileri açığa çıkarmayacaklarını garanti edecek şekilde düzenlenir.

9.7. Sorumlulukların Geçersiz Olduğu Durumlar

İlgili değildir.

9.8. "ESHS"nin Sorumluluğun Sınırlandırılması

"e-tuğra"nın sorumlulukları yalnızca sertifikalarda bulunan kullanım ve maddi kapsama ilişkin sınırlamalar ve sertifika kullanıcı sözleşme ve/veya taahhütnamelerinde belirtilen sorumluluklar ile sınırlıdır.

9.9. Tazminatlar

Sertifika sahiplerinin kullanıcı sözleşmeleri uyarınca yükümlülüklerini yerine getirmedikleri durumlarda, "e-tuğra"nın, kurumsal başvuru sahiplerinin veya üçüncü kişilerin zarar görmesi halinde, sertifika sahipleri bu zararları tazminle mükelleftir.

Kurumsal başvuru sahiplerinin Kurumsal Başvuru Sözleşmesi uyarınca yükümlülüklerini yerine getirmedikleri durumlarda, "e-tuğra"nın, sertifika sahiplerinin veya üçüncü kişilerin zarar görmesi halinde, kurumsal sertifika sahipleri bu zararları tazminle mükelleftir.

"e-tuğra" "Kanun" ve ilgili mevzuattan kaynaklanan veya "SUE" ve "Sİ"de yer alan ilke ve esaslar gereği yükümlülüklerini yerine getirmediği resmi olarak ispatlandığı takdirde, sertifika sahiplerinin ve üçüncü kişilerin bu durumdan kaynaklanan ve resmi olarak ispatlanmış zararlarını tazminle mükelleftir.

Sertifika sahipleri, sertifika sahibi taahhütnamesi veya anlaşması hükümleri ve "Sİ" ve "SUE" dokümanlarında yer alan hükümler gereği yükümlülüklerini yerine getirmez ve bu durumdan "e-tuğra" veya üçüncü kişiler zarar görürse, ilgili zararın sertifika sahibi tarafından tazmin edilmesi gerekir.

9.10. "Sİ"nin Geçerliliği ve Sona ermesi

9.10.1. "Sİ" dokümanının Geçerlilik Dönemi

İşbu "Sİ", "e-tuğra" bilgi bankasında yayınlandığı zaman geçerliliği başlar, dökümanın yeni bir sürümü çıkana kadar geçerli kalır.

9.10.2. "Sİ" dokümanının Geçerliliğinin Sona Ermesi

İşbu "SUE", yeni sürümünün yayınlanmasından itibaren geçerliliğini yitirir.

9.10.3. Geçerliliğin Sona Ermesinin Etkileri ve İşlerliğin Sürdürülmesi

"e-tuğra", "e-tuğra" Bilgi Deposu aracılığıyla "Sİ"nin geçerliliğini yitirmesi ile oluşacak etkileri web sitesi aracılığı ile duyurur. Her koşulda, gizli bilgilerin korunması ile ilgili sorumlulukları devam eder. Tüm Kullanıcı Sözleşmeleri sertifikanın iptal edilmesine veya geçerlilik süresinin sonuna kadar geçerlidir. Yeni "Sİ" sürümü, eski "Sİ" sürümünün geçerliliği sona ermeden hazırlanır ve değişiklik hizmet kesintisi olmadan gerçekleştirilir "Sİ" güncellemeleri gereği üretilen sertifikalarda herhangi bir değişiklik yapılması gerekirse, sertifika sahipleriyle ve üçüncü kişilerle bu durum paylaşılır ve gerekli işlemler yapılır.

9.11. Bireysel Bildirimler ve Katılımcılar Arasında İletişim

"e-tuğra" ile sertifika sahipleri ve kurumsal başvuru sahipleri ile arasındaki iletişim eposta, telefon veya yazı ile yapılır. Sertifika sahipleri Bölüm 1.5.2'de belirtilen irtibat bilgilerini kullanarak "e-tuğra" ile iletişime geçer.

Toplu veya üçüncü kişiler ile yapılacak duyurular "e-tuğra" web sitesi üzerinden, e-posta veya veya yazılı olarak gerçekleştirilir.

"e-tuğra" gerekli görmesi durumunda kullanıcı sözleşmelerine iletişim ile ilgili notlar ve maddeler ekleyebilir.

9.12. Değişiklikler

Sertifika İlkeleri (Sİ), mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısında değerlendirilir. Bu değerlendirmeler ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçık güncellenir.

"Sİ" dokümanın yayınlanan sürümünde herhangi bir değişiklik yapılması gerektiğinde, değişikliklerin yansıtıldığı yeni "Sİ" dokümanı "e-tuğra" bilgi güvenliği forumu onayından geçtikten sonra yeni bir sürüm olarak yayımlanır.

Yeni sürümde "Sİ" dokümanının bir önceki sürümünde yer alan işleyişe göre üretilmiş sertifikaları etkilemeyecek değişikliklerin olacağı gibi etkileyebilecek şekilde değişiklikler de olabilir. Sertifika kullanımlarını etkileyen değişikliklerde "e-tuğra" gerekli tedbirleri alır.

9.12.1. Değişiklik Prosedürü

Sertifika İlkeleri (Sİ) ve Sertifika Uygulama Esasları (SUE) kitapçıkları mevzuat ve standartlar çerçevesinde en az yılda bir kere Yönetim Gözden Geçirme Toplantısında değerlendirilir. Bu değerlendirmeler ya da yıl içinde ortaya çıkabilecek gereklilikler doğrultusunda bu kitapçıklar güncellenir.

"e-tuğra" faaliyetlerinde herhangi bir değişiklik veya güncelleme olduğunda e- Tuğra bu değişiklikleri "Sİ" ve "SUE" dokümanında güncelleyerek, yeni sürüm olarak yayınlanacaktır.

"Sİ" dokümanında herhangi bir değişiklik veya güncelleme olduğunda da "SUE" dokümanını da ilgilendiren bölümler güncellenir. "SUE" dokümanı da yeni bir sürüm olarak yayımlanır. "SUE" dokümanı ve ilgili uygulamalar, yönetim gözden geçirme toplantılarında yıllık olarak gözden geçirilir.

"Sİ" ve "SUE" dökümanın da etkisi küçük değişiklikler olması durumunda, güncelleme tarihinden önce verilmiş olan sertifikalar da yeni "Sİ" ve "SUE" sürümüne göre kullanılmaya devam eder. Önemli değişiklikler nedeniyle yeni bir "Sİ" sürümü çıkarılmış ise, güncelleme tarihinden önce üretilmiş sertifikaların, değişiklik yapılan sertifika ilkelerine bağlı olanları, yeni "Sİ" ve ilgili "SUE"ye uyumlu olarak kullanılamayabilir.

9.12.2. Duyuru Mekanizması ve Süresi

Yeni "Sİ" ve "Sİ" sürümleri, eski sürümlerle birlikte "e-tuğra" bilgi deposunda, sürüm bilgisi içerecek ve ilgili tüm tarafların erişimine açık tutulacak şekilde yayımlanır.

İhbarda Bulunulmadan Değiştirilebilecek Maddeler

"e-tuğra" "Sİ" kapsamında bulunan ilgililerin hak ve yükümlülüklerin de değişiklik yaratmayacak nitelikte olan "Sİ" değişikliklerini ve/veya düzeltmelerini önceden ihbarda bulunmadan web sitesinden yayınlayarak yapar.

"e-tuğra" işleyişinin güvenliği ile ilgili durumlarda "Sİ" ve "SUE" üzerinde gerekli değişiklikleri herhangi bir ihbar veya bildirimde bulunmadan yapmaya yetkilidir. Bu durumlarda yapılan değişiklikler, değişiklik ve düzeltmenin bilgi deposunda yayınlanmasından sonra yürürlüğe girer.

İhbarda Bulunarak Değiştirilebilecek Maddeler

"e-tuğra", "Sİ" kapsamında bulunan ilgililerin hak ve yükümlülüklerin de değişiklik yaratacak nitelikte olan değişikliklerini ve/veya düzeltmeleri, değişiklik ve/veya düzeltmenin önemine göre belirleyeceği bir süre öncesinde öneri/taslak olarak bildirir.

"e-tuğra" öneri/taslak bildirimlerini sertifika sahiplerine ve diğer ilgililere web sitesinden duyuru ile gerçekleştirir. "e-tuğra" belirlediği süre içerisinde öneri/taslak metnine ilgililerden gelen yorumları dikkate alarak gerekli değişiklikleri yapar ve değişiklik ve/veya düzeltmeleri bilgi deposunda yayınlayarak yürürlüğe koyar.

9.12.3. Nesne Tanımlayıcı Numaralarının Değişmesini Gerektiren Durumlar

"e-tuğra" tarafından yeni bir sertifika uygulama alanında kullanılmak üzere yeni bir sertifika ilkesi dokümanı yayınlanması veya ilgili sertifika ilkelerinin nesne tanımlayıcı numaralarının da değişmesi gerekliliği durumunda bu sertifika alanında kullanılacak yeni üretilen sertifikalarda, uygulanacak olan yeni sertifika ilkelerinin nesne tanımlayıcı numaraları yer alır.

9.13. Anlaşmazlıkların Çözümü

Sulh: "e-tuğra", sertifika sahipleri ve üçüncü kişiler ile arasında oluşabilecek anlaşmazlık, sorun ve görüş ayrılıkları husule gelmesi durumunda, her iki taraf da diğer tarafa yazılı olarak sorun ile ilgili bilgi aktaracak ve iyi niyetle konuyu ortak bir anlaşma zemini oluşturarak "Sİ" ve "SUE" kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler, taahhütnameler ve sözleşmeler uyarınca çözmeye çalışacaktır. Nitelikli elektronik sertifikalarla ilgili işlemler Kanun, Yönetmelik ve Tebliğler uyarınca yürütülür.

Uzlaştırma: Bir tarafın diğerine göndereceği yazıyla bu çabaların sonuçsuz kaldığı, uyuşmazlığın ortaya çıktığı tarihten 1 (bir) ay içerisinde belgelendiği takdirde, bu defa tarafların avukatları, Avukatlık Kanunu md. 35/A'daki yetkilerine istinaden "Sİ" ve "SUE" kitapçıklarında belirlenmiş ilke ve uygulama esasları ile prosedürler, taahhütnameler ve sözleşmeler uyarınca tarafları uzlaştırmaya çalışacaklardır. Nitelikli elektronik sertifikalarla ilgili anlaşmazlıklar da ilgili Kanun , Yönetmelik ve Tebliğler geçerlidir.

Tahkim: Tarafların avukatlarının uzlaştırma çabaları sonuç vermezse, uyuşmazlıkların çözümü için Ankara Mahkemeleri yetkilidir.

9.14. Yasal Düzenleme

"Sİ"nin yorumlanmasında, 5070 sayılı Elektronik İmza Kanunu ile ilgili Yönetmelik ve Tebliğler temel alınır.

"Sİ"nin uygulanmasında ve yorumlanmasında Türk Cumhuriyeti Hukuku geçerlidir.

9.15. İlgili Yasalara Uygunluk

"e-tuğra" "NES" hizmetlerini, 5070 sayılı Elektronik İmza Kanunu ile ilgili Yönetmelik, Tebliğ ve diğer düzenlemelere uygun olarak gerçekleştirir ve yürütür.

9.16. Çeşitli Hükümler

9.16.1. Bütün sözleşme

İlgili değildir.

9.16.2. Devir ve Temlik

İlgili değildir.

9.16.3. Bölünebilirlik

"Sİ"nin herhangi bir bölümünün kalıcı veya geçici olarak geçersiz sayılması veya geçerliliğini kaybetmesi durumunda bu bölümden etkilenmeyen diğer bölümler geçerliliğini korur.

9.16.4. Yaptırımlar (Yasal Haklardan Feragat)

İlgili değildir.

9.16.5. Mücbir Sebep

Mücbir sebep hallerinde "e-tuğra" "Sİ"den doğan yükümlülüklerini yerine getiremeyebilir. Savaş, seferberlik, doğal afetler, yangın, telekomünikasyon hatlarında meydana gelen problemler, dürüstlük kuralı gereğince ifa talep etmenin karşı taraf için çok büyük bir idari ve mali külfet getirecek biçimde mevzuatta yapılan değişiklikler gibi "e-tuğra"nın ilgili faaliyetlerini yerine getirmesini engelleyecek ve normal koşullar altında kontrol edilebilir olmayan durumlar mücbir sebep olarak kabul edilir.

9.17. Diğer Hükümler

İlgili değildir.