e-Güven
Sertifika Uygulama Esasları
(Nitelikli Elektronik Sertifika Dışındaki Elektronik Sertifikalar için)

Sürüm 1.0

Yürürlük Tarihi: Temmuz, 2009

OID
2.16.792.3.0.1.1.3.1

Elektronik Bilgi Güvenliği Anonim Şirketi
Halk Sokak, No:35, Golden Plaza, F Blok, Kat:2,Daire 6
Sahrayıcedit
İstanbul

Tel : 0-216-360 46 05
Fax: 0-216-360 33 56
www.e-guven.com

e-Güven Sertifika Uygulama Esasları

Açıklamalar ve Uyarılar

Bu dokümanda kullanılan markalar Elektronik Bilgi Güvenliği A.Ş. veya ilgili tarafların mülkiyetindedir.

Yukarıda belirtilen haklar saklı kalmak kaydıyla ve aşağıda özel olarak aksine izin verilen durumlar hariç olmak üzere, bu yayının hiçbir parçası, önceden Elektronik Bilgi Güvenliği A.Ş.'nin izni alınmadan herhangi bir formda veya herhangi bir araçla (elektronik, mekanik, fotokopi, kayıt veya başka araçlar) çoğaltılamaz, aktarılamaz ya da bir veri okuma sistemine kaydedilemez veya işlenemez.

Bununla birlikte, (i) yukarıdaki telif hakkı uyarısının ve giriş paragraflarının her bir nüshanın başında açıkça gösterilmesi ve (ii) bu dokümanın, Elektronik Bilgi Güvenliği A.Ş.'ye atıf yapılarak, bir bütün halinde ve hatasız kopyalanması şartıyla, bu eserin ücreti ödenmeden çoğaltılmasına ve dağıtılmasına izin verilebilir. Bununla birlikte çoğaltma ve dağıtım izni herhangi bir kişiye münhasıran verilmez.

e-Güven Sertifika Uygulama Esasları (SUE); IETF RFC 3647 standartına uygun olarak hazırlanmıştır. İşbu SUE ile ilgili yorum ve uyuşmazlıklar taraflar arasındaki cari hukuki ilişkiyi tesis eden ve yöneten sözleşme, belge, taahhütname veya beyan gibi hukuki enstrümanlar kullanılarak değerlendirilecek ve çözüme kavuşturulacaktır.

İÇİNDEKİLER

1. Giriş

Bu doküman e-Güven Sertifika Uygulama Esasları'dır (SUE). SUE İnternet Mühendisliği Görev Grubu'nun (IETF) elektronik sertifika ilkeleri ile ilgili standartı olan IETF RFC 3647 standartına uyumlu olacak şekilde hazırlanmıştır.

e-Güven sertifika ilkeleri; e-Güven'in sertifikaların düzenlenmesi, yönetilmesi, askıya alınması, iptal edilmesi ve yenilenmesi de dahil olmak ve fakat bunlarla sınırlı olmamak üzere sertifikalandırma hizmetlerinin sunumunda kullandığı uygulamaları açıklayan ve e-Güven'in politikasını belirleyen belgelerdir. SUE; nitelikli elektronik sertifikalar dışında e-Güven'in yayınladığı elektronik sertifikalar için, sertifika ilkelerinin çizdiği çerçeve içerisinde, e-Güven'in uygulamalarını sertifika sahiplerine ve üçüncü kişilere detaylı bir şekilde açıklamaktadır.

e-Güven, 5070 Sayılı Elektronik İmza Kanunu hükümleri çerçevesinde elektronik sertifika, elektronik imza ve zaman damgası hizmetlerini sunan bir Elektronik Sertifika Hizmet Sağlayıcısı'dır; ancak işbu dokümanla belirlenen kural ve koşullar e-Güven tarafından yayınlanan nitelikli elektronik sertifikalar dışındaki elektronik sertifikalar için düzenlenmiştir.

1.1 *Genel*

e-Güven, ilgili mevzuattaki gereksinimleri yerine getirerek Telekomünikasyon Kurumu'na bildirimde bulunmuş ve gerekli yetkiye sahip bir "***Elektronik Sertifika Hizmet Sağlayıcısı (ESHS)***"dır. e-Güven'in 5070 Sayılı Elektronik İmza Kanunu ve ilgili mevzuat hükümleri uyarınca yürüttüğü hizmetlerle ilgili kural ve koşullar e-Güven Nitelikli Elektronik Sertifika Uygulama Esasları belgesi içerisinde belirtilmektedir. İşbu SUE ile e-Güven'in nitelikli elektronik sertifika hizmetleri dışında vermiş olduğu diğer hizmetler ve bu hizmetlere bağlı açık anahtar sertifikalarına ilişkin kural ve koşullar tanımlanmaktadır.

e-Güven, nitelikli elektronik sertifika dışında yayınladığı elektronik sertifikaların uygulama alanlarını, elektronik sertifika otorietesi olarak işleyişini ve yükümlülüklerini açıkladığı sertifika ilkeleri belgelerini ve sertifika ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan e-Güven Sertifika Uygulama Esasları (SUE) belgesini yayımlar.

1.2 *Tanımlama*

e-Güven Sertifika Uygulama Esasları için belirteç;

e-Güven Sertifika Uygulama Esasları Sürüm 1.0

2.16.792.3.0.1.1.2.1

e-Güven SSL Elektronik Sertifika İlkeleri için belirteç;

e-Güven SSL Sertifika İlkeleri 1.0

2.16.792.3.0.1.1.1.2

1.3 *Katılımcılar*

İşbu SUE kapsamındaki katılımcılar, e-Güven'in sağladığı hizmetlerde ve ESHS fonksiyonlarını yerine getirmesinde hizmet alan ve hizmetlerin yerine getirilmesinde görev alan taraflardır.

1.3.1 Elektronik Sertifika Hizmet Sağlayıcısı - ESHS (e-Güven)

ESHS 5070 Sayılı Elektronik İmza Kanunu ve ilgili mevzuat kapsamında belirtilen iş ve işlemleri yerine getiren bir yapı olmasının yanında, nitelikli elektronik sertifika dışında elektronik sertifika hizmetleri sağlayan ve elektronik sertifikaların yaşam döngüsünü yöneten birimi tanımlamak amacıyla kullanılmaktadır.

e-Güven sertifika zinciri yapısı; e-Güven Kök Sertifika Hizmet Sağlayıcısı Sertifikası, bu sertifika tarafından imzalanmış ve altında yer alan e-Güven Mobil Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı Sertifikası ve e-Güven Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı ve e-Güven SSL Sertifika Hizmet Sağlayıcısı Sertifikası şeklindedir. MKNESİ kapsamına giren ve Mobil İmza için kullanılan nitelikli elektronik sertifikalar (NES) e-Güven Mobil Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı Sertifikası ile imzalanır. Bunun dışındaki NES'ler ise e-Güven Nitelikli Elektronik Sertifika Hizmet Sağlayıcısı Sertifikası ile imzalanır. SSL sertifikaları ise e-Güven SSL Sertifika Hizmet Sağlayıcısı Sertifikası ile imzalanır.

1.3.2 Kayıt Makamları

NES dışındaki elektronik sertifika kayıt işlemleri sadece ESHS tarafından yapıldığı için düzenlenmesine gerek görülmemiştir.

1.3.3 Sertifika Sahipleri

1.3.3.1 SSL Sertifikası Sahibi

SUE kapsamında SSL Sertifikası Sahibi, SUE ile belirlenen prosedürlerle ilgili şart ve koşulları yerine getirerek SSL sertifikası başvurusu yapmış ve e-Güven tarafından kendisine SSL sertifikası tahsisi edilmiş kişilerdir.

1.3.3.2 Güvenlik Sertifikası Sahibi

SUE kapsamında Güvenlik Sertifikası Sahibi SUE ile belirlenen prosedürlerle ilgili şart ve koşulları yerine getirerek güvenlik sertifikası başvurusu yapmış ve e-Güven tarafından kendisine güvenlik sertifikası tahsisi edilmiş kişilerdir.

1.3.4 Üçüncü Kişiler

İşbu dokümanda üçüncü kişiler, e-Güven tarafından yayınlanmış NES dışındaki elektronik sertifikalara dayanarak ve güvenerek menfi ve müspet açıdan iş ve işlemlerde bulunan gerçek ve tüzel kişilerdir. Sertifika Sahipleri aynı zamanda üçüncü kişi de olabilirler.

1.3.5 Diğer Katılımcılar

1.3.5.1 Politika Yönetim Otoritesi

PYO, e-Güven'in aşağıdaki konularda yönetim ve sorumluluğa sahip güvenli personelden oluşan yetkili birimidir;

- e-Güven altyapısını ve uygulamalarını belirlemek ve onaylamak,
- Sertifika ilkelerini ve SUE'yi onaylamak,
- Sertifika ilkeleri ve SUE'nin gözden geçirme ve yenilenme prosedürlerini belirlemek,
- e-Güven'in ESHS olarak işleyişinde görev alan süjelerin sertifika ilkelerine ve SUE'ye göre faaliyetlerini kontrol etmek
- SUE'nin sertifika ilkelerine uygunluğunu denetlemek,

1.3.5.2 Güven Merkezi

Güven Merkezi, e-Güven'in ESHS operasyonlarını içersindeki sertifika otoritesi ve zaman damgası hizmet sağlayıcısı fonksiyonlarını yerine getiren çekirdek birimidir. Güven Merkezi, TS ISO/IEC 27001 güvenlik sertifikasına sahip olarak bilgi güvenliği yönetimini bu sertifikasyonda belirtilen gerekliliklere uygun olarak yerine getirmektedir. Güven Merkezi, e-Güven in tescilli şirket merkezi dışındaki güvenli bir alanda; iş ve işlemlerini bu merkez sınırları içersinde geçerli olan standartlara, 5070 Sayılı Kanun ve ilgili mevzuat hükümlerine uygun olarak yürütmekte ve yerine getirmektedir. Güven Merkezi, en üst düzeyde teknik, personel ve fiziki güvenlik prosedürlerine uyar. Güven Merkezi içersinde yürütülen faaliyetler gizlidir; bu tür hususlar üçüncü kişilerin bilgisinden uzaktır. e-Güven Güven Merkezi içersinde yürütülen operasyonlar, personel bilgileri ve süreçler konusunda sadece hukuken yetkili olan resmi makamlara açıklamada bulunmakla yükümlüdür.

1.4 Sertifika Kullanımı

1.4.1 İzin Verilen Sertifika Kullanımı

e-Güven tarafından oluşturulan SSL sertifikaları sunucu ve istemci arasında gerçekleştirilen iletişimde klimk doğrulama ve şifreli iletişim amacıyla kullanılırlar.

e-Güven tarafından oluşturulan güvenlik sertifikaları verilerin şifrelenmesi ve kimlik doğrulama amacıyla kullanılırlar.

1.4.2 Yasaklanan Sertifika Kullanımı

e-Güven tarafından oluşturulan SSL sertifikaları ve güvenlik sertifikaları SUE 1.4.1'de belirtilen amaçlar dışında kullanılamayacaktır.

1.5 Politika Yönetimi

1.5.1 SUE ile ilgili Yetkili Kurum

İşbu SUE'nin idaresi e-Güven Politika Yönetim Otoritesi tarafından yürütülmektedir.

1.5.2 İletişim Noktası

e-Güven Politika Yönetim Otoritesi'ne iletilecek sorular için aşağıdaki adres kullanılmalıdır:

Elektronik Bilgi Güvenliği Anonim Şirketi

Halk Sokak No:35, Golden Plaza
F Blok, Kat:2, Daire 6 34734
Sahrayıcedit / Kadıköy / İstanbul
Tel: (216) 360 46 05
Fax: (216) 360 33 56

1.5.3 SUE'nin Politikaya Uygunluğunu Belirleyen Kişi

PYO; SUE'nin, sertifika ilkelerine uygunluğunu denetlemekten sorumludur.

1.5.4 SUE Onaylama Prosedürü

e-Güven uzmanları tarafından yapılan çalışmalar ve ilgili taraflardan gelen talepler doğrultusunda SUE'de değişiklik ve gerektiğinde yenileme taslakları oluşturulur. Onaylanmaya hazır duruma getirilen taslaklar PYO'nun onayına sunulur. PYO uygun görmesi halinde taslakları onaylar.

1.6 Tanımlar ve Kısaltmalar

Tanımlar ve kısaltmalar için EK-A'ya bakınız.

2. Yayınlama ve Bilgi Deposu Sorumlulukları

2.1 Bilgi Deposu

e-Güven yayınladığı elektronik sertifikalar, SİL'ler, sertifika ilkeleri, SUE, kullanıcı sözleşmeleri ve bilgilendirici dokümanlar için bilgi deposu fonksiyonlarını yerine getirir. Bilgi deposu elektronik sertifika sahiplerinin, üçüncü kişilerin ve ilgili herkesin erişimine 7/24 hizmet verecek şekilde erişime açık bulundurulur.

2.2 Sertifika Bilgilerinin Yayınlanması

e-Güven aşağıdakiler için veri depolama işlevinden sorumludur:

- e-Güven Kök Sertifika Hizmet Sağlayıcısı Sertifikası
- e-Güven SSL Sertifika Hizmet Sağlayıcısı Sertifikası
- Zaman Damgası ve ÇSDP Sertifikaları
- Sertifika sahibinin izin vermesi durumunda sertifika sahibi adına e-Güven tarafından düzenlenen sertifikaları
- Sertifika İptal Listeleri
- NESUE
- SUE
- Sertifika İlkeleri
- Kullanıcı Sözleşmeleri
- Bilgilendirici dokümanlar

2.3 Yayınlanma Sıklığı

- SUE'de yapılan güncellemeler ve Kullanıcı Sözleşmelerinde yapılan değişiklikler SUE 9.12'e göre yayınlanır.
- Sertifikalar düzenlendikleri tarihte yayınlanır.
- İptal durum kayıtları SUE 4.9.7 ve 4.9.10'e göre yayınlanır.

e-Güven yayınlama hizmetini kesintisiz olarak (7/24) verir.

2.4 Bilgi Deposu Erişim Kontrolleri

e-Güven web sitesinin veri tabanı kullanılarak yayınlanan bilgiler herkese açık bilgilerdir. Bu bilgilere salt okunur erişim sınırsızdır. e-Güven, sertifika durum bilgisine veya SİL'lere erişim koşulu olarak SUE'de yer alan hükümlerin kabul edilmesini öngörür. e-Güven, yetkisiz kişilerin veri tabanına erişerek veri tabanında yer alan bilgiler üzerinde çeşitli ekleme, silme veya değişiklik yapmasını önlemek için mantıksal ve fiziksel güvenlik önlemleri almıştır.

3. Tanımlama ve Kimlik Doğrulama

3.1 İsimlendirme (İlk Kayıt)

3.1.1 İsim Tipleri

e-Güven Kök Sertifikası, Düzenleyen ve Konu alanlarında X.501 Özgün İsim içerir. e-Güven Kök Sertifikası Özgün İsimleri aşağıdaki tabloda belirtilen elemanlardan oluşur.

Özellik	*Değer*
Ülke (C) =	TR
Kurum (O) =	Elektronik Bilgi Guvenligi A.S.
Ortak İsim (CN) =	e-Guven KoK Sertifika Hizmet Saglayicisi

e-Güven SSL Sertifika Hizmet Sağlayıcısı Sertifikası (SSL Kök Sertifikası) Düzenleyen ve Konu alanlarında X.501 Özgün İsim içerir. e-Güven SSL Kök Sertifikası Özgün İsimleri aşağıdaki tabloda belirtilen elemanlardan oluşur.

Özellik	*Değer*
Ülke (C) =	TR
Kurum (O) =	Elektronik Bilgi Guvenligi A.S.
Ortak İsim (CN) =	e-Guven SSL Sertifika Hizmet Saglayicisi

SUE kapsamındaki güvenlik sertifikaları, konu ismi alanında bir X.501 özgün ismi içerir ve aşağıdaki tablolarda belirtilen elemanlardan oluşur.

Güvenlik sertifikası	
Özellik	*Değer*
Ülke (C) =	TR
Ortak İsim (CN) =	Güvenlik sertifikası sahibinin adı ve soyadı
Kurum (O) =	Elektronik Bilgi Güvenliği A.Ş.
Seri Numarası (Serial Number)	T.C. Kimlik Numarası / Pasaport Numarası

SUE kapsamındaki SSL sertifikaları, konu ismi alanında bir X.501 özgün ismi içerir ve aşağıdaki tablolarda belirtilen elemanlardan oluşur.

Güvenlik sertifikası	
Özellik	*Değer*
Ülke (C) =	TR
Ortak İsim (CN) =	Güvenlik sertifikası sahibinin adı ve soyadı
Kurum (O) =	Elektronik Bilgi Güvenliği A.Ş.
Seri Numarası (Serial Number)	T.C. Kimlik Numarası / Pasaport Numarası

3.1.2 İsimlerin Anlamlı Olması Gerekliliği

Güvenlik sertifikaları, sertifika sahibi olan bireyin kimliğinin belirlenmesine olanak sağlayan, genelde bilinen anlamlara sahip isimler içerir.

SSL sertifikaları, sertifika sahibi olan kurumun kimliğinin belirlenmesine olanak sağlayan tüzel kişi adını ve kurumun web sitesinin adını içerir.

e-Güven Kök Sertifika Hizmet Sağlayıcısı Sertifikası, sadece "e-Guven Kok Sertifika Hizmet Saglayicisi" ismine sahiptir.

e-Güven SSL Sertifika Hizmet Sağlayıcısı Sertifikası, sadece "e-Guven SSL Sertifika Hizmet Saglayicisi" ismine sahiptir.

3.1.3 Sertifika Başvurusunda Bulunan Kişilerin İsimlerini Gizlemesi veya Takma İsim Kullanımı

SUE kapsamındaki sertifikalarda takma isim kullanılmamaktadır.

3.1.4 Değişik İsim Tiplerini Yorumlamak İçin Kurallar

Koşul yoktur.

3.1.5 İsimlerin Benzersizliği

e-Güven farklı gerçek ve tüzel kişilere ait sertifikalardaki kimlik bilgilerinin benzersiz olmasını sağlar.

3.1.6 Tanımlama, Doğrulama ve Markaların Rolü

Sertifika başvurularında başkalarının fikri mülkiyet haklarını ihlal eden isimler kullanmaları yasaktır. e-Güven, sertifika başvurusunda gösterilen isim üzerinde fikri mülkiyet hakkı bulunup bulunmadığını kontrol etmez ya da herhangi bir alan adı, ticaret ünvanı, isim, ticari marka, hizmet markası veya servis işaretinin mülkiyetiyle ilgili herhangi bir ihtilafta hakemlik veya aracılık yapmaz ya da bu ihtilafı herhangi bir şekilde çözmeye çalışmaz. e-Güven, sertifika sahibine sorumluluk yüklemeksizin, bu tip bir ihtilaftan dolayı herhangi bir sertifika başvurusunu reddetmeye veya askıya almaya yetkilidir.

3.2 İlk Kimlik Doğrulaması

3.2.1 İmza Oluşturma Verisinin Zilyetliğinin Kanıtlanması Metodu

e-Güven, Sertifika sahibinin bir imza oluşturma verisine sahip olduğunu, PKCS #10'la veya şifreleme açısından eşdeğer başka bir kanıtla veya e-Güven onaylı başka bir yöntemle doğrular.

3.2.2 Tüzel Kişilerin Kimliğinin Doğrulanması

Tüzel kişilere verilecek SSL sertifikalarında sertifika başvuru sahibinin kimliği ticari sicil kaydı, imza sürküleri gibi resmi belgeler aracılığıyla doğrulanır. Bunların yanı sıra elektronik posta bilgisi kullanıcıya kontrol amaçlı gönderilen e-posta'ya yanıt alınması ile doğrulanır.

3.2.3 Gerçek Kişilerin Kimliğinin Doğrulanması

e-Güven, sertifika başvurusunda bulunan gerçek kişilerin kimlik bilgilerini nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere dayanarak, kimlik bilgileri dışında sertifika içersinde yer alacak diğer bilgileri ise e-Güven tarafından belirlenen resmi belgelere dayanarak kontrol eder. Bunların yanı sıra elektronik posta bilgisi kullanıcıya kontrol amaçlı gönderilen e-posta'ya yanıt alınması ile doğrulanır.

3.2.4 Doğrulanmayan Başvuru Bilgileri

Koşul yoktur.

3.2.5 Sertifika Sahibinin Bağlı Olduğu Kurumlarla İlişkisinin Kanıtlanması

Bkz. SUE 3.2.2

3.2.6 Karşılıklı İşlerlik Kriterleri

e-Güven'in mevcut uygulamasında karşılıklı işlerlik içerisinde olduğu başka bir ESHS yoktur. e-Güven başka bir ESHS ile karşılıklı işlerlik sağladığında bu hususu tüm ilgili taraflara duyuraacaktır.

3.3 Yeniden Anahtarlama için Tanımlama ve Kimlik Doğrulama

Sertifika sahipleri sertifikanın geçerlilik süresi sona ermeden önce sertifika yenileme talebinde bulunabilirler. Böyle bir yenileme talebinde SUE 3.2.2 ve 3.2.3 ile belirlenen kimlik doğrulama prosedürleri uygulanır.

3.3.1 Rutin Yeniden Anahtarlama için Tanımlama ve Kimlik Doğrulama

Rutin yeniden anahtarlama talebinde SUE 3.2.2 ve 3.2.3 ile belirlenen kimlik doğrulama prosedürleri uygulanır.

3.4 İptal Talebi İçin Tanımlama ve Kimlik Doğrulama

Sertifika iptal talebinde bulunan kimse e-Güven Çağrı Merkezi'ni arayarak iptal talebinde bulunur ve sertifika iptal talebinde bulunan kimsenin kimliği ve iptal talebinde bulunma yetkisi doğrulanır.

Sertifika iptal talebinin alınmasından sonra, e-Güven tarafından sertifika sahibinden onay alınıncaya kadar sertifika askıya alınır. Sertifika iptal talebi, iptal talebinde bulunan kişinin kimlik bilgilerinin tespit edilmesi ve güvenlik soruşturmasından geçmesi sonucunda alınmışsa gerekli onay alınmış sayılır ve derhal iptal edilir. İptal edilen sertifika geçerlilik süresi sonuna kadar SİL'de yer alır.

4. Sertifika Yaşam Zinciri Operasyonel Gereklilikler

4.1 Sertifika Başvurusu

4.1.1 Kim Sertifika Başvurusunda Bulunabilir

Tüm gerçek ve tüzel kişiler SUE ile belirlenen şartları sağlamaları ve ilgili prosedürleri yerine getirmeleri koşuluyla sertifika başvurusunda bulunabililer.

4.1.2 Kayıt Süreci ve Sorumluluklar

e-Güven sertifikaları için yapılan başvurularda kayıt süreci için aşağıdaki prosedürler uygulanır;

- Sertifika başvuru sahibinin e-Güven'le Kullanıcı Sözleşmesini akdetmesi
- Sertifika başvuru sahibinin kimlik doğrulama prosedürlerinin SUE 3.2'de belirtilen şekilde yerine getirilmesi,

4.2 Sertifika Başvuru Süreci

4.2.1 Tanımlama İşlemi ve Kimlik Kanıtlama Fonksiyonları

e-Güven SUE 3.2'de belirtilen yöntemlerle tanımlama ve kimlik kontrolü yapmak zorundadır.

4.2.2 Sertifika Başvurularının Kabulü ve Reddi

e-Güven aşağıdaki koşulların sağlanması halinde sertifika başvurularını kabul ederler;

- SUE 3.2'de belirtilen tanımlama ve kimlik kontrolü prosedürlerinin eksiksiz olarak yerine getirilmiş olması,
- Kullanıcı Sözleşmesinin imzlanmış olması
- Sertifika ücretinin ödenmiş olması

e-Güven aşağıdaki durumlarda sertifika başvurularını reddederler;

- SUE 3.2'de belirtilen tanımlama ve kimlik kontrolü prosedürlerinin eksiksiz olarak yerine getirilmemiş olması,
- Sertifika başvurusunda bulunan kişinin kendisinden istenen bilgi ve belgeleri eksiksiz olarak temin etmemiş olması,
- Sertifika başvurusunbulunan kendisine tebliğ edilen ihtarlara veya bildirimlere zamanında cevap vermemesi veya bahsi geçen ihtar ve bildirimdeki hususları yerine getirmemiş olması,

4.2.3 Sertifika Başvuru Süreci Zamanlaması

e-Güven sertifika başvurularına ilgili sözleşmelerde özel bir hüküm bulunmaması halinde mümkün olan en kısa zamanda cevap verecektir.

4.3 Sertifika Yayınlanması

4.3.1 Sertifika Yayınlanması Esnasında ESHS'nin Faaliyetleri

e-Güven yapılan başvuruların değerlendirilmesi ve değerlendirmenin başarılı olması üzerine başvuru sahiplerine başvuru belgelerindeki ilgili bilgileri içeren sertifikaları yayınlar.

4.3.2 Sertifika Başvurusunda Bulunan Kişiye Sertifikayı Yayınlayan ESHS Tarafından Yapılan Bildirim

Sertifika başvuru sahiplerine sertifikanın yayınlanmasından sonra sms, e-posta, telefon veya faks aracılığıyla bildirimde bulunulur.

4.4 Sertifikanın Kabulü

4.4.1 Sertifikanın Kabulü Sayılan İşlemler

Sertifika sahibi kendisine sertifikanın yaratıldığına ilişkin bildirimin yapılmasının ardından ivedilikle sertifikasını kontrol edecektir. Sertifika sahibinin, sertifika içerisinde yer alan bilgilerle, sertifika başvurusu sırasında teslim ettiği belgeler içerisindeki bilgiler arasında farklılık olduğunu tespit etmesi durumunda derhal sertifika iptal talebinde bulunacaktır. Sertifika sahibinin makul süreler içerisinde böyle bir talepte bulunmaması sertifikanın kabulü sayılacaktır.

4.4.2 ESHS Tarafından Sertifikaların Yayınlanması

e-Güven sertifikaları kamuya açık bir dizinde yayınlar.

4.4.3 Diğer İlgililere ESHS Tarafından Sertifika Yayınlanmasına ilişkin Yapılan Bildirim

Koşul yoktur.

4.5 İmza Oluşturma/Doğrulama Verileri ve Sertifika Kullanımı

4.5.1 Sertifika Sahiplerinin İmza Oluşturma Verisi ve Sertifika Kullanımı

Sertifika sahipleri imza oluşturma verilerini ve sertifikalarını, SUE, ilgili sertifika ilkeleri ve imzalamış oldukları kullanıcı sözleşmeleri ile belirlenen yükümlükleri doğrultusunda kullanmak zorundadırlar. Sertifika sahipleri; imza oluşturma ve doğrulama verilerini sadece sertifikanın anahtar kullanım alanı içerisinde belirtilen amaçlar dahilinde kullanabilirler. Sertifika sahibi imza oluşturma verisinin ve erişim verisinin güvenliğini sağlamak ve izinsiz kullanımlarını engellemekle yükümlüdür. Sertifika sahibi, 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 ESHS'yi bilgilendirmelidir.

4.5.2 Üçüncü Kişilerin İmza Doğrulama Verisi ve Sertifika Kullanımı

Sertifikaya güvenerek iş ve işlem yapacak olan üçüncü kişiler öncelikle elektronik imza ile bağlı ile olan sertifikanın kontrolünü yapmalıdırlar. Sertifikaya ilişkin kontoller; sertifikanın e-Güven tarafından yayınlandığının kontrolü (sertifikanın e-Güven Kök ve ESHS sertifikaları ile imzalanmış olmasından), sertifikanın geçerlilik süresi içerisinde olduğunun kontrolü, sertifikanın iptal veya askıya alınmadığının kontrolü şeklindedir. Üçüncü kişiler sertifika kontrolünün ve doğrulama prosedürlerinin başarısız olması durumunda sertifikaya dayanarak işlem yapmamalıdır.

4.6 Sertifika Yenileme

Sertifika yenileme, sertifikanın imza oluşturma ve doğrulama verileri değiştirilmeden yenilenmesidir. e-Güven sertifikaları imza oluşturma ve doğrulama verileri değiştirilmeden yenilenmezler, e-Güven sertifikaları sadece yeniden anahtarlama ile yenilenirler.

4.6.1 Sertifika Yenileme Koşulları

Koşul yoktur.

4.6.2 Sertifika Yenileme Başvurusunda Kimler Bulunabilir

Koşul yoktur.

4.6.3 Sertifika Yenileme Taleplerinin İşleyiş Süreci

Koşul yoktur.

4.6.4 Yeni Sertifika Yayınlanmasının Sertifika Yenileme Başvurusunda Bulunan Kişiye Bildirimi

Koşul yoktur.

4.6.5 Sertifika Yenilemenin Kabulü Sayılan İşlemler

Koşul yoktur.

4.6.6 ESHS Tarafından Yenilenen Sertifikanın Yayınlanması

Koşul yoktur.

4.6.7 Diğer Tarafların Yenilenen Sertifika ile ilgili Bilgilendirilmesi

Koşul Yoktur

4.7 Sertifikanın Yeniden Anahtarlanması

Sertifikanın yeniden anahtarlanması, sertifikanın imza oluşturma ve doğrulama verilerinin değiştirilerek yenilenmesidir.

4.7.1 Sertifikanın Yeniden Anahtarlanmasını Gerektiren Durumlar

Sertifikanın geçerlilik süresinin sona ermesinden önce sertifikanın geçerliliğini sürdürebilmek için sertifikanın yeniden anahtarlama yoluyla yenilenmesi gerekir.

4.7.2 Kimler Yeni İmza Doğrulama Verisinin Sertifikalanması İçin Talepte Bulunabilirler

Yenileme talebinde bulunan sertifika sahipleri yeni imza doğrulama verisinin sertifilanması için talepte bulnabilirler.

4.7.3 Sertifikanın Yeniden Anahtarlanmasına Yönelik Taleplerin İşleyişi

Bkz. SUE 3.3.1

4.7.4 Yeniden Anahtarlama Talebinde Bulunanlara Yeni Sertifika Yayınlama Bildiriminin Yapılması

SUE 4.3.2'ye uygun olarak yeniden anahtarlama ile sertifikası yenilenen sertifika sahibine ve kurumsal başvuru sahibine bildirim yapılır.

4.7.5 Sertifikanın Yeniden Anahtarlanmasının Kabulü Sayılan İşlemler

SUE 4.4.1'e göre yapılan işlemler yeniden anahtarlama ile yenilenmiş sertifikanın kabulü sayılır.

4.7.6 ESHS Tarafından Yeniden Anahtarlanan Sertifikanın Yayınlanması

Yeniden anahtarlama ile yenilenen sertifikalar e-Güven tarafından kamuya açık bir dizinde yayınlanır.

4.7.7 Diğer İlgililere Sertifika Yayınlanmasına İlişkin ESHS Tarafından Yapılan Bildirim

Koşul yoktur.

4.8 Sertifikalar Üzerinde Yapılan Değişiklik

4.8.1 Sertifikalarda Değişiklik Yapılmasını Gerektiren Durumlar

Sertifiikanın içeriğinin değiştirilmesi ancak sertifika iptal edilmesi ve yeni bir sertifikanın oluşturulması ile gerçekleşebilir. Bu tür bir değişiklik yeni bir sertifika başvuru sürecinin başlatılmasını gerektirir.

4.8.2 Kimler Sertifikada Değişiklik Yapılmasını Talep Edebilir

Koşul yoktur.

4.8.3 Sertifika Üzerinde Değişiklik Yapılmasına İlişkin Taleplerin Süreci

Koşul yoktur

4.8.4 Yeni Sertifika Yayınlanmasına İlişkin Sertifika Başvurusunda Bulunanlara Yapılan Bildirim

Koşul yoktur.

4.8.5 Değiştirilmiş Sertifikaların Kabulü Sayılan İşlemler

Koşul yoktur.

4.8.6 ESHS Tarafından Sertifika Değişikliklerine İlişkin Yayın

Koşul yoktur.

4.8.7 ESHS Tarafından Diğer Kuruluşlara Sertifika Yayınlanmasına İlişkin Bildirim

Koşul yoktur.

4.9 Sertifika İptali ve Askıya Alma

e-Güven sertifika iptal ve askıya alma prosedürleri ile ilgili olarak aşağıdaki garantileri verir;

- İptal edilen sertifika, geçerlilik süresi sonuna kadar Sertifika İptal Listesi'nde (SİL) yer alır.
- e-Güven, SİL'leri herhangi bir kimlik doğrulamasına gerek olmaksızın ücretsiz ve kesintisiz olarak kamu erişimine açık tutar. Kayıtların bir sonraki güncelleme zamanı SİL'lerde açıkça gösterilir.
- e-Güven, sertifikaları geçmişe yönelik olarak iptal etmeyecektir.
- Sertifika iptal edildiği takdirde yenilenemez ancak gerekli prosedürler yerine getirilerek yeniden oluşturulur.
- SİL her 3 saatte bir 24 saat geçerli olacak şekilde yenilenir.
- Askıya alma ve iptal hizmetleri 7/24 (haftada 7 gün, günde 24 saat) olmak üzere hizmete açık olacaktır. e-Güven'in kontrolü dışında sistemin arızalanması veya hizmetin aksaması durumunda, e-Güven bu aksamaların veya arızaların 24 saatten fazla sürmemesi için elinden gelen tüm çabayı sarf edecektir.
- Sertifika iptal listeleri (SİL) 7/24 (haftada 7 gün, günde 24 saat) olmak üzere erişime açık olacaktır. e-Güven'in kontrolü dışında sistemin arızalanması veya hizmetin aksaması durumunda, e-Güven bu aksamaların veya arızaların 24 saatten fazla sürmemesi için elinden gelen tüm çabayı sarf edecektir.
- SİL'lerin bütünlüğü ve tanımlanması, SİL'lerin e-Güven tarafından, ESHS Sertifikası ile elektronik olarak imzalanması sonucu sağlanacaktır.

4.9.1 Sertifika İptalinin Şartları

Sertifikalar aşağıdaki koşullarda iptal edilir:

- e-Güven tarafında, ve/veya herhangi bir kimsede, sertifika sahibinin imza oluşturma verisiyle ilgili bir tehdit bulunduğu yönünde bir kanaat veya güçlü bir şüphe oluşması.
- Sertifika sahibinin sözleşmeden ve ilgili mevzuattan doğan yükümlülüklerini yerine getirmemesi, sertifika sahibinin güvenlikle ilgili yeterli önlemleri almaması
- e-Güven, ve/veya sertifika sahibinde, sertifika başvurusundaki bir maddi durumun yanlış olduğu yönünde kanaat oluşturan bir sebebin ortaya çıkması.
- Sertifika yayınlama ile ilgili bir esaslı önşartın yerine getirilmediği veya bu şarttan feragatin gerçekleştirilmediğinin tespiti.
- Sertifikada bulunan bilgilerin yanlış veya değiştirilmiş olması.
- Sertifika sahibinin veya sertifika iptali ile yetkili bir kişinin sertifikanın iptalini talep etmesi.
- Sertifikada bulunan bilgilerin geçerliliğini yitirmesi
- Yukarıda sayılanlara ek olarak; Kullanıcı Sözleşmesinde sertifikanın iptali ile ilgili hükümlerde belirtilen şartlardan birinin gerçekleşmesi.

4.9.2 Kimler İptal Başvurusunda Bulunabilir

Seritifika sahibi, e-Güven, yetkili kamu kuruluşları ve yargı makamları sertifikanın iptal edilmesini talep edebilir

4.9.3 İptal Başvurusuna İlişkin Talepler

Sertifika için iptal talebi e-Güven telefon destek hattı aranarak veya ilgili sertifika ilkeleri içerisinde belirtilen yöntemlerle yapılabilir.

4.9.4 İptal Başvurusuna İlişkin Değerlendirme Süreci

Sertifika iptal talebinde bulunan kimse e-Güven Çağrı Merkezi'ni arayarak iptal talebinde bulunur ve sertifika iptal talebinde bulunan kimsenin kimliği ve iptal talebinde bulunma yetkisi doğrulanır.

Sertifika iptal talebinin alınmasından sonra, e-Güven tarafından sertifika sahibinden onay alınıncaya kadar sertifika askıya alınır. Sertifika iptal talebi, iptal talebinde bulunan kişinin kimlik bilgilerinin tespit edilmesi ve güvenlik soruşturmasından geçmesi sonucunda alınmışsa gerekli onay alınmış sayılır ve derhal iptal edilir.

4.9.5 ESHS'nin İptal Talebini İşleme Koyma Süresi

Sertifika iptal talepleri hemen işleme alınır. Sertifika iptal talebinin onaylanmasından sonra sertifika ilk yayınlanacak SİL'de yer alır ve bu süre 3 saati geçmez.

4.9.6 İptal Durumuna İlişkin Üçüncü Kişilerin Kontrol Yükümlülüğü

Üçüncü kişiler bir sertifikaya güvenerek işlem yapmak için sertifikanın iptal durumunu kontrol etmelidirler. Üçüncü kişiler iptal durumunun kontrolü için; SİL veya Çevrimiçi Sertifika Durum Protokolü kontrolü yöntemlerinden birini seçmek zorundadırlar.

4.9.7 İptal Durum Kaydı Yayınlama Sıklığı

e-Güven, iptal edilen ve askıya alınan sertifikalarını gösteren SİL'leri yayınlar ve durum kontrol servisleri sunar. GKNESİ ve MKNESİ kapsamı dışındaki SİL'ler 3 saatte bir 24 saat geçerli olacak şekilde yenilenir.

4.9.8 SİL'deki Güncellemelerin SİL'e Yansıma Zamanı

SİL'ler yaratılmalarının ardından yayınlandıkları dizine en kısa sürede yollanmaktadır; bu süreç otomatik olarak birkaç dakika içerisinde gerçekleşmektedir.

4.9.9 Çevrimiçi İptal Kontrolü Erişilebilirliği

e-Güven, SİL'leri yayınlamasının yanı sıra e-Güven veri bankasında sorgulama işlevleriyle sertifika durum bilgisi sunma hizmeti ve Çevrimiçi Sertifika Durum Protokolü hizmeti de verir.

4.9.10 Çevrimiçi İptal Kontrolü Gereklilikleri

Bkz. SUE 4.9.6

4.9.11 İptal Duyurularının Diğer Biçimlerine Erişilebilirlik

Koşul yoktur.

4.9.12 ESHS İmza Oluşturma ve Doğrulama Verilerinin Yenilenmesinde Özel Gereksinimler

e-Güven kendi imza oluşturma ve doğrulama verilerinin yenilenmesini gerektiren durumlarda üçüncü kişileri bilgilendirmek için elinden gelen çabayı sarf edecektir.

4.9.13 Askı Koşulları

Sertifikanın belirli bir süre kullanım dışı bırakılmak istenmesi, imza oluşturma ve doğrulama verilerinin güvenliği ile ilgili şüpheye düşülmesi gibi sebeplerle sertifikanın askıya alınması talebinde bulunulabilir. Askıya alma, iptalden farklı olarak geriye dönülebilir bir işlemdir. İptal edilen sertifikalar yeniden geçerlilik kazanamazken, askıya alınmış sertifikalar askı durumundan çıkartılarak yeniden geçerlilik kazanabilir. Sertifikalar iptal edilmeden önce gerekli onay süreçleri için de askıya alınabilir.

4.9.14 Kimler Askı Talebinde Bulunabilir

Seritifika sahibi, e-Güven, yetkili kamu kuruluşları ve yargı makamları sertifikanın askıya alınmasını talep edebilir.

4.9.15 Askı Talebi Süreci

Sertifikalar için askıya alma talebi, e-Güven telefon destek hattı aranarak veya ilgili sertifika ilkeleri içerisinde belirtilen yöntemlerle yapılabilir.

4.9.16 Askı Süresindeki Limitler

a. İptal talebinde: Sertifika iptal talebinden sonra, 10 gün içerisinde e-Güven tarafından sertifika iptali ile ilgili onaylama soruşturması yapılmalıdır. Soruşturma süresinin sonunda elde edilen sonuca göre sertifika askı durumu kaldırılır veya sertifika iptal edilir.
b. Askıya alma talebinde: Sertifika askıya alma talebinden sonra sertifika geçerlilik süresinin sonuna kadar askıda kalabilir.

4.10 *Sertifika Durum Hizmetleri*

4.10.1 Operasyonel Özellikler

Sertifikaların durumları ile ilgili bilgiler SİL'ler veya Çevrimiçi Sertifika Durum Protokolü kontrolü kullanılarak alınabilir.

4.10.2 Hizmet Erişilebilirliği

Sertifika durum bilgileri hizmetleri haftada yedi gün yirmi dört saat (7/24) kesintisiz olarak verilmektedir. e-Güven'in kontrolü dışında sistemin arızalanması veya hizmetin aksaması

durumunda, e-Güven en fazla 24 saat içerisinde hizmetlerin tekrar sağlanabilmesi için elinden gelen tüm çabayı sarf edecektir.

4.10.3 Seçimlik Özellikler

Koşul yoktur.

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-Güven, sertifika sahipleri için imza oluşturma verisi saklama hizmeti vermemektedir.

4.12.1 İmza Oluşturma Verisi Kurtarma ve Yedekleme Politikası ve Esasları

Koşul yoktur.

4.12.2 Oturum Anahtarı Sarma (Encapsulation) ve Kurtarma Politikası ve Uygulamaları

Koşul yoktur.

5. Kaynaklar, Yönetim ve Operasyonel Kontroller

5.1 Fiziksel Kontroller

5.1.1 Güven Merkezi Konumu ve İnşası

Bütün e-Güven ESHS operasyonları, gizli veya açık müdahaleleri durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan bir Güven Merkezi içinde yürütülür.

e-Güven ile yaptığı özel sözleşme ile kendi bünyesinde sistem kurulan kurumsal başvuru sahipleri ve kayıt makamları kendi bünyelerinde yürütecekleri operasyonlarla ilgili güvenli tesislerinin, kendileri ile yapılan sözleşmede belirtilen güvenlik şartlarını karşılamasını sağlamalıdır.

5.1.2 Fiziksel Erişim

e-Güven ESHS sistemleri ve Güven Merkezi, “Fiziksel ve Çevresel Güvenlik Prosedürü” doğrultusunda çeşitli fiziksel güvenlik seviyeleriyle korunur . Yüksek bir seviyeye sahip bir alana veya sisteme erişim yapılmadan önce alçak seviyelere erişilmelidir.

Her katmana erişim fiziksel erişim kontrolleri aracılığı ile gerçekleşir. Her katmana erişim sadece güvenli personele ait olan güvenlik kartlarıyla gerçekleşir. Tüm fiziksel erişim hareketleri otomatik olarak kaydedililr ve video ile de görüntüsel kayıt altına alınır. İleri katmanlara erişim biyometrik tanımlamanın da kullanıldığı iki faktörlü doğrulama kontrolüyle gerçekleşir. Güvenli personel özelliğine sahip olmayan personelin veya ziyaretçilerin refakatsiz olarak güvenli alanlara girmesine izin verilmemektedir. İmza oluşturma verisi cihazlarına ve yan ürünlerine erişim yetkilerin ayrımı kurallarının gereğince yerine getirilir.

5.1.3 Elektrik ve Klima Koşulları

e-Güven'in güvenli tesisleri aşağıdaki sistemlere ait ana ve yedek sistemlerle donatılmıştır:

- Elektrik gücüne sürekli ve kesintisiz erişim sağlamak için elektrik sistemleri.
- Sıcaklığı ve nispi nemi kontrol etmek için ısıtma/havalandırma/klima sistemleri.

5.1.4 Suya Karşı Korunma

Güven Merkezi, su baskınları ve sele karşı gerekli yalıtım sistemleri ve su dedektörleri ile korunmakta ve izlenmektedir.

5.1.5 Yangın Önlemleri ve Korunması

Güven Merkezi, yangınları veya hasara yol açan diğer alev veya duman vakalarını önlemek ve söndürmek için yangın alarmları, ısı dedektörleri ve yangın söndürme sistemleri ile donatılmıştır.

5.1.6 Veri Araçları Saklanması

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

5.1.7 Atık Kontrolü

e-Güven ESHS işleyişi uyarınca kayıtları tutulan tüm organizasyonel bilgiler, süreleri geldiğinde imha edilirler. Elektronik kayıtların yetkili olmayan kişiler tarafından görülmesi, değiştirilmesi ve/veya silinmesi önlenmiştir. Kağıt üzerinde bulunan kayıtlar ise sadece yetkili kişilerin girme izni bulunan özel birimlerde tutulurlar. Yedekleme prosedürü uyarınca tüm kayıtlar yedeklenir. Kağıt ya da elektronik ortamda saklanan tüm bilgi ve belgeler saklanmaları gerekmiyorsa "Kayıt İmha Prosedürü"ne göre imha edilir. Kriptografik modüller atılmaları gerektiğinde ya fiziksel olarak imha edilir ya da üretici firma talimatları doğrultusunda sıfırlanır.

5.1.8 Arka Plan Yedeklemesi

e-Güven, kritik sistem verilerini, denetim kaydı verilerini ve diğer gizli bilgileri "İş Sürekliliği ve Felaketten Kurtarma Planı" çerçevesinde rutin olarak yedekler.

5.2 *Prosedür Kontrolleri*

5.2.1 Güvenli Personel

Sertifika yaşam zinciri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, ESHS sertifika yönetim sistemleri ve veri bankaları kontrolleri, gerekli erişim ve kontrol yetkisine sahip güvenli personel tarafından yürütülür. Güvenli personel, faaliyet alanlarına göre; elektronik imza teknolojisi, bilgi güvenliği ve risk yönetimi konularında yeterli bilgi ve tecrübe seviyesine sahip kişilerden seçilir. Güvenli personel tanımları aşağıdaki şekildedir;

- Güven Merkezi ve Güvenlik Yöneticisi: Güvenlik sistemininin tüm politika ve prensiplerinin belirlenmesi, uygulanması, onaylanması görev, yetki ve sorumluluğuna sahip güvenli personel

- Sistem Denetçisi : ESHS güvenli sistemlerinin denetim kayıtlarına ve arşivlerine erişme ve devamlılığını sağlama görev ve yetkisine sahip güvenli personel

- Güven Merkezi Sistem Yöneticisi : Sertifika başvuruları yönetimi, sertifika oluşturulması, güvenli elektronik imza oluşturma araçları yönetimi, sertifika iptal yönetimi için kullanılan ESHS güvenli sistemlerini kurma, konfigüre etme ve bakımını yapma görev ve yetkisine sahip güvenli personel

- Güven Merkezi İşletim Sistemi ve Veritabanı Yöneticisi: Güven Merkezi'nde koşan yazılımların üzerinde koştuğu işletim sisteminin ve veritabanlarının konfigüre edilmesi, yönetilmesi; bunların tuttukları kayıtların ve arşivlerin işletilmesi görev ve yetkisine sahip güvenli personel

- Güven Merkezi Ağ Yöneticisi: Güven Merkezi ağ yapısının yönetilmesi, kullanıcı ihlallerinin tespiti ve raporrlanması görev ve sorumluluğuna sahip personel

- Kayıt Makamı (RA) Sistem İşletmenleri: Sertifikaların oluşturulması, iptali, askıya alınması konularında onaylama görev ve yetkisine sahip güvenli personel.

- Güven Merkezi Sistem İşletmenleri : ESHS güvenli sistemlerini günlük bazda kullanma, sistem yedeklemesi ve kurtarma fonksiyonlarını kullanma görev ve yetkisine sahip güvenli personel

Güvenli personel, "Personel Prosedürü" doğrultusunda SUE 5.3'deki kriterleri yerine getiren kimseler arasından; Güven Merkezi ve Güvenlik Yöneticisi veya e-Güven Genel Müdürü tarafından seçilir ve görevlendirilir.

5.2.2 Her Bir Görev için Gereken Kişi Sayısı

e-Güven, görevlerin sorumluluklara göre ayrılmasını sağlamak için sıkı kontrol prosedürleri uygular. ESHS şifreleme donanımına (kriptografik imzalama ünitesi veya CSU) ve ilgili anahtar malzemesine erişim gibi en hassas görevler birden fazla güvenilen şahıs gerektirir.

Bu dahili kontrol prosedürleri, cihaza fiziksel veya mantıksal erişime sahip olmak için en az iki güvenilen personelin gerekli olmasını sağlayacak şekilde tasarlanmıştır. ESHS şifreleme donanımına erişim, ilk alındığı ve kontrolden geçirildiği andan son mantıksal ve/veya fiziksel imhaya kadar donanımın ömrü boyunca daima birden fazla güvenilen şahısla sağlanır. Bir modül, işlem kodlarıyla devreye alındığında, cihaza hem fiziksel, hem de mantıksal erişim üzerinde ikili kontrol sağlamak için süreklilik arz eden erişim kontrolleri uygulanır.

5.2.3 Her Bir Görev için Tanımlama ve Kimlik Kontrolü

Güvenli personel, yetkileri doğrultusunda gerçekleştirecekleri faaliyetleri için tanımlama kontrollerine tabi tutulurlar. Tanımlama kontrolleri için güvenli personelin kimlik ve biyolojik bilgileri alınarak güvenlik sistemine kaydedilir.

5.2.4 Sorumlukların Ayrılmasını Gerektiren Roller

Bazı sertifika sertifika yaşam zinciri işlemleri, ESHS anahtar yönetimi işlemleri ve bunlara ilişkin kontroller birden çok güvenli personelin katılımıyla ve sorumlulukların ayrıştırılması prensibiyle gerçekleştirilir.

5.3 Personel Kontrolleri

5.3.1 Mesleki Bilgi, Nitelikler, Deneyim ve Resmi Makam İzinlerinin Şartları

Güvenli personel olmak isteyen kişiler, görev sorumluluklarını gerektiği gibi ve tatmin edici şekilde yerine getirmesi için gereken mesleki bilgi, nitelik ve deneyimlerini kanıtlayan belgeleri sunmalıdır.

e-Güven'in, kurucu ortakları, tüzel kişiliği temsile yetkili yöneticileri ve istihdam ettiği veya ettirdiği personeli; taksirli suçlar hariç olmak üzere, affa uğramış olsalar bile ağır hapis veya altı (6) aydan fazla hapis yahut basit veya nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, inancı kötüye kullanma, dolanlı iflas gibi yüz kızartıcı suçlar ile istimal ve istihlak kaçakçılığı dışında kalan kaçakçılık suçları, resmi ihale ve alım satımlara fesat karıştırma, kara para aklama veya devlet sırlarını açığa vurma, vergi kaçakçılığı ya da iştirak veya bilişim alanındaki suçlar nedeniyle hüküm giymemiş olacaktır.

İşe kabul edilen personel ile karşılıklı gizlilik ve işe alım anlaşmaları imzalanır, personelin T.C vatandaşı olması veya T.C 'de ikamet ve çalışma izni almış olması, herhangi bir resmi ya da özel kuruluşa karşı hizmet yükümlülüğü bulunmaması gerekmektedir.

5.3.2 Mesleki Bilgi Kontrol Prosedürleri

Personel bir güvenilen konumda çalışmaya başlamadan önce, e-Güven, aşağıdakileri içeren mesleki bilgi kontrolleri yapar:

- Önceki işinin doğrulanması
- Mesleki referansın kontrolü
- Adli sicil soruşturması
- Vergi ve vatandaşlık numarası

Bir mesleki bilgi kontrolünde ortaya çıkan ve güvenilen şahıs adaylarının reddedilmesine yol açan ya da mevcut bir güvenilen şahsa karşı belirli bir hareket tarzının uygulanması için zemin oluşturduğu düşünülebilecek faktörler genel olarak aşağıda sıralanmaktadır:

- Aday veya güvenilen şahsın hatalı veya yanıltıcı beyanlarda bulunması.
- Büyük ölçüde olumsuz veya güvenilir olmayan kişisel referanslar.

5.3.3 Eğitim Şartları

Güvenli personel mesleki sorumluluklar, güvenlik prosedürleri ve politikaları konularında gerekli hukuki ve teknik eğitimden geçirilirler. Güvenli personel eğitim programları periyodik olarak gözden geçirilir ve gerekli görüldüğünde güncellenir.

5.3.4 Eğitim Sıklığı ve Şartları

e-Güven, personeline, iş sorumluluklarını gerektiği gibi ve tatmin edici düzeyde yerine getirmesi ve gerekli uzmanlık seviyesini muhafaza etmesini sağlamak için gereken ölçüde ve sıklıkta bilgi güncelleme eğitimi verir. Periyodik güvenlik bilinci eğitimi devamlı olarak verilmektedir.

5.3.5 İş Rotasyon Sıklığı ve Sırası

Koşul yoktur.

5.3.6 Yetkisiz Eylemlere Karşı Yaptırımlar

Yetkisiz eylemler veya e-Güven politikalarının ve prosedürlerinin başka şekillerde ihlali durumunda gereken disiplin önlemleri alınır. Yetkisiz eylemler veya prosedür ihlali fiilleri Elektronik İmza Kanunu, Türk Ceza Kanunu veya ilgili diğer kanunlarda belirtilen suç tanımlarına dahil olması durumunda bu eylemleri gerçekleştirenler hakkında gerekli yasal işlemler yapılır.

5.3.7 Sözleşmeli Personel Şartları

e-Güven gerekli durumlarda, ESHS faaliyetleri veya diğer faaliyetleri için bağımsız yükleniciler veya danışmanlar kullanılabilir. Bilgü güvenliği kapsamına giren konularda faaliyet gösteren yükleniciler, yüklenicilerin çalışanları veya danışmanlar, eşdeğer konumdaki e-Güven personeliyle aynı mesleki koşullara ve güvenlik koşullarına tâbi tutulur.

5.3.8 Personele Verilen Dokümanlar

e-Güven personeli ve yüklenici personeline, faaliyetleri doğrultusunda öğrenmeleri gereken gizli bilgiler dışında, yetkileri doğrultusunda kullandıkları donanım ve yazılıma ilişkin dokümanları, e-Güven TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dokümanları (yüklenici personeli eğer varsa yüklenicinin bilgi güvenliği yönetim sistemi dokümanlarına sahip olacaklardır), NESUE, SUE, sertifika ilkeleri, ZDUE ve ZDİ belgeleri verilir.

5.4 *Denetim ve Kayıt Prosedürleri*

5.4.1 Kaydedilen Olay Tipleri

e-Güven aşağıdaki önemli olayları manuel veya otomatik olarak kaydeder:

- ESHS imza oluşturma ve doğrulama verisi yaşam döngüsü yönetimi olayları:
  - Anahtar (veri) yaratma, yedekleme, saklama, kurtarma, arşivleme ve imha etme.
  - Şifreleme cihazı periyodu yönetimi olayları.

- ESHS ve sertifika yaşam döngüsü yönetimi olayları:
  - Sertifika başvuruları, yenileme, yeniden anahtarlama ve iptal.
  - Başarılı veya başarısız talep işlemleri.
  - Sertifikaların ve SİL'lerin yaratılması ve yayınlanması.

- Güvenlikle ilgili olaylar:
  - e-Güven personelinin güvenlik sistemi eylemleri.
  - Sistem arızaları, donanım arızaları ve diğer anormallikler.
  - Güvenlik duvarı ve rooter aktivitesi.
  - ESHS Güven Merkezi tesisi ziyaretçi girişi/çıkışı.

5.4.2 Kayıt İşleme Sıklığı

Denetim kayıtları, en azından haftada bir önemli güvenlik ve operasyonel olaylar açısından kontrolden geçirilmelidir.

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 SUE 5.5.2'ye göre arşivlenir.

5.4.4 Denetim Kaydının Korunması

Elektronik ve manuel denetim kaydı dosyaları, yetkisiz kişilerin izlemesi, değişiklik yapması, silmesi veya başka herhangi bir şekilde erişimine karşı fiziksel ve mantıksal erişim kontrolleri kullanılarak korunur.

5.4.5 Denetim Kaydı Yedekleme Prosedürleri

Denetim kayıtları her gün kademeli olarak yedeklenir ve haftada bir de tam yedekleme yapılır.

5.4.6 Denetim Bilgisi Toplama Sistemi

Başvuru safhasında, ağ ve işletim sistemi seviyesinde denetim verileri otomatik olarak yaratılır ve kaydedilir. Manuel olarak yaratılan denetim verileri e-Güven personelince manuel olarak kaydedilir.

5.4.7 Olaya Sebep Olan Sertifika Sahibine veya İlgiliye İhbarda Bulunma

Denetim bilgisi toplama sistemi bir olay kaydettiği zaman, olaya sebep olan birey, kurum, cihaz veya başvuruya ihbarda bulunmaya gerek yoktur. Güvenlik sistemi içerisinde önemli güvenlik ihlalleri, ilgili güvenli personele e-mail ve/veya cep telefonu aracılığıyla sistem tarafından bildirilir.

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*

e-Güven, SUE 5.4'de belirtilen denetim kayıtlarına ilave olarak sertifika başvurularına ve sertifika sahiplerine, ESHS ve diğer katılımcılar arasındaki bütün veri iletişimine ilişkin olarak kayıt tutar.

5.5.1 Kaydedilen Olay Tipleri

- Sertifika başvuruları
- Kullanıcı Sözleşmeleri ve ilgili diğer sözleşme ve belgeler
- Sertifikaların yaratılması, düzenlenmesi, kullanılması, iptali, sona ermesi ve yeniden anahtarlanması ya da yenilenmesiyle ilgili eylem ve bilgiler (eylemlerin zamanı ve eylemleri yapan yetkililer de dahil olmak üzere)
- e-Güven tarafından sağlanan sertifikaların içerikleri
- Geçerlilik süresi sona eren sertifikaları,
- Geçerlilik süresinin sona ermesinden itibaren e-Güven ESHS sertifikasını
- e-Güven ESHS yeniden anahtarlama bilgileri
- İptal, askıya alma, askıdan kaldırma ile ilgili talep ve talebin doğrulanması eylemleri ve ilgili iletişim bilgileri
- Zaman damgalarını
- SİL'leri
- e-Güven tarafından yayınlanan sertifika ilkeleri, sertifika uygulama esasları, zaman damgası uygulama esaslarını ve zaman damgası ilkelerini

- e-Güven tarafından yapılan denetleme sonuçları

Kayıtlar, doğru ve tam olarak sıralanması, saklanması, korunması ve çoğaltılması şartıyla elektronik veya basılı kopya halinde tutulabilir.

5.5.2 Arşiv Saklama Periyodu

e-Güven 5.5.1'de belirtilen kayıtları en az 20 yıl süreyle saklar.

5.5.3 Arşivin Korunması

e-Güven, SUE 5.5.1 altında derlenmiş arşiv kayıtlarını sadece yetkili kişilerin arşivlenmiş verilere erişmesine izin verecek şekilde korur. Elektronik olarak arşivlenmiş veriler, uygun fiziksel ve mantıksal erişim kontrolleri kullanılarak, yetkisiz izleme, değiştirme, silme veya başka herhangi bir şekilde erişime karşı korunur. Arşivlenmiş verilerin tutulduğu araçlar ve bunları işlemek için gereken başvurular saklanarak, arşivlenmiş verilere SUE 5.5.2'de belirtilen süreler içinde erişilebilmesi sağlanır.

5.5.4 Arşiv Yedekleme Prosedürleri

e-Güven, düzenlenen sertifika bilgisiyle ilgili elektronik arşivleri her gün kademeli olarak yedekler ve haftada bir de tam yedekleme yapar.

5.5.5 Kayıtlara Zaman Damgası Basma Şartları

Sertifikalar, SİL'ler ve diğer iptal veri tabanı girdileri zaman ve tarih bilgisi içerir.

5.5.6 Arşiv Toplama Sistemi

Arşivler elektronik ortamda veya yetkili kişilerin sorumluluğunda manuel olarak toplanır.

5.5.7 Arşiv Bilgisine Ulaşma ve Doğrulama Prosedürleri

e-Güven ESHS işleyişiyle ilgili bilgi ve belgeler http://www.e-guven.com/e-imza/bilgideposu adresinde yayınlanmaktadır. Ancak güvenlik prosedürleri ile ilgili belgeler sadece e-Güven güvenli personeli tarafından erişilebilecektir. Sertifika sahiplerinin kimlik bilgilerine ise sadece güvenli personel erişebilecektir. Arşivde bulunan belgeler saklanma süresi boyunca okunabilir bir formatta tutulacaktır.

5.6 *İmza Oluşturma – Doğrulama Verileri (Anahtar) Değiştirme*

e-Güven ESHS imza oluşturma ve doğrulama verileri ilgili mevzuatta belirtildiği üzere en fazla 10 yıl olabilir. Sertifika kullanıcıları için geçerlilik süresinin 1 yıl olması halinde e-Güven ESHS sertifikalarının sertifikaları onaylama işlevini kaybetmemesi için e-Güven ESHS sertifikalarının geçerlilik süresinin sona erme tarihinden en azından 13 ay önce yenilenmesi gerekmektedir.

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 ve Felaketten Kurtarma Planı" 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 ve Felaketten 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 ilgili taraflara bilgi verilir.

5.7.3 ESHS İmza Oluşturma Verisinin Zarar Görmesi

e-Güven ESHS imza oluşturma verileri ve doğrulama verileri ile aktivasyon verilerinin yedekleri farklı lokasyonda çevrimdışı ortamlarda felaket anında kullanılmak üzere güvenli personel kontrolünde muhafaza edilmektedir.

5.7.4 İş Sürekliliği

"İş Sürekliliği ve Felaketten Kurtarma Planı" doğrultusunda işleyişi engelleyecek olaylar karşısında ortaya konacak eylem ve işlemler belirlenir.

5.8 *ESHS'nin Operasyonunun Durdurulması*

e-Güven'in ESHS faaliyetlerini durdurması gerektiği durumlarda, ESHS operasyonları durdurulmadan önce son kullanıcıları, kurumsal başvuru sahiplerini, üçüncü kişileri ve diğer ilgili kuruluşları bundan haberdar etmek için ticari açıdan gerekli her türlü çabayı gösterir. Operasyonun durdurulması kararının verilmesinden sonra e-Güven ESHS işleyişinde kendisine yardımcı olan bağlı kişi ve kuruluşlarla olan sözleşmelerini sonlardır.

6. Teknik Güvenlik Kontrolleri

6.1 *İmza Oluşturma ve Doğrulama Verilerini Yaratma ve Kurma*

6.1.1 İmza Oluşturma ve Doğrulama Verilerini Yaratma

ESHS imza oluşturma ve doğrulama verileri yaratma işlemi, yaratılan veriler için güvenliği ve gerekli şifreleme gücünü temin eden güvenilir sistemler kullanılarak, önceden seçilmiş birden fazla güvenli personel tarafından yerine getirilir. e-Güven Kök ve Alt Kök ESHS Sertifikaları için, imza oluşturma ve doğrulama verileri yaratmada kullanılan şifreleme modüllerinin bileşenleri FIPS 140-2 Seviye 3 şartlarını karşılar.

ESHS imza oluşturma ve doğrulama verileri, önceden planlanmış "Anahtar Yaratma Prosedürü"nde belirtilen şartlara göre yaratılır. Her bir anahtar yaratma prosedüründe yapılan faaliyetler kaydedilir, tarih atılır ve imzalanır. Bu kayıtlar denetim ve izleme amacıyla, PYO'nun uygun gördüğü süreyle saklanır.

6.1.2 Sertifika Sahibine İmza Oluşturma Verisinin Verilmesi

Sertifika imza oluşturma ve doğrulama verileri tipik olarak sertifika sahibi tarafından yaratılır; bu nedenle, bu gibi durumlarda sertifika sahibine imza oluşturma verisi verilmesi söz konusu değildir.

6.1.3 ESHS'ye İmza Doğrulama Verisinin Verilmesi

Sertifika sahipleri bir PKCS#10 sertifika imzalama talebi (CSR) veya başka dijital imzalı paket kullanarak sertifika için imza doğrulama verilerini e-Güven'e verirler.

6.1.4 Kullanıcılara ESHS İmza Doğrulama Verilerinin Verilmesi

e-Güven, ESHS imza doğrulama verilerini de içeren ESHS sertifikaları http://www.e-guven.com/e-imza/bilgideposu adresinden indirilebilir.

6.1.5 İmza Oluşturma ve Doğrulama Verilerinin Büyüklüğü

e-Güven ESHS imza oluşturma ve doğrulama verileri, 2048 bit RSA büyüklüğündedir.

6.1.6 İmza Doğrulama Verisi Parametrelerinin Yaratılması ve Kalite Kontrolü

Koşul yoktur.

6.1.7 Anahtar Kullanım Amaçları (Her Bir X.509 v 3 Tipi Sertifikanın "Anahtar Kullanımı" Başlığındaki Alanı İçersinde)

e-Güven ESHS sertifikalarının anahtar kullanım alanları "sertifika imzalama" ve "CRL imzalama" alanlarına ayarlanır.

6.2 *İmza Oluşturma Verisinin Korunması ve Şifreleme Modülü Sistem Kontrolleri*

6.2.1 Şifreleme Modülü Standartları ve Kontrolleri

e-Güven, ESHS imza oluşturma ve doğrulama verilerini yaratma işlemleri için FIPS 140-2 Seviye 3 onaylı bileşenlere sahip donanım şifreleme modülleri kullanır.

6.2.2 İmza Oluşturma Verisi (n* m) Birden Fazla Kişi Kontrolü

e-Güven ESHS sertifikalarının imza oluşturma verilerinin kullanılmasını gerektiren işlemler en az iki güvenli personelin katılımıyla ve gerekli tanımlama ve güvenlik kontrollerinin yerine getirilmesiyle gerçekleştirilir.

6.2.3 İmza Oluşturma Verisinin Saklanması

e-Güven, ESHS imza oluşturma verisini, resmi makamların erişimi amacıyla dahi olsa herhangi bir üçüncü şahsa vermez.

e-Güven, seertifika sahiplerinin imza oluşturma verilerinin kopyalarını saklamaz.

6.2.4 İmza Oluşturma Verisi Yedekleme

e-Güven, rutin ve felaketten kurtarma amaçlarıyla ESHS imza oluşturma verilerinin yedek kopyalarını oluşturur. Bu veriler, Güven Merkezi dışındaki güvenli bir lokasyonda saklanır.

e-Güven, sertifika sahiplerinin imza oluşturma verilerini yedeklemez.

6.2.5 İmza Oluşturma Verisi Arşivleme

e-Güven ESHS imza oluşturma ve doğrulama verileri arşivlenmez.

6.2.6 İmza Oluşturma Verisinin Kriptografik Modül Transferi

e-Güven, ESHS imza oluşturma ve doğrulama verileri, verilerin kullanılacağı donanım şifreleme modüllerinde (ESHS güvenli elektronik imza oluşturma aracı) yaratır. e-Güven, ayrıca, rutin ve felaketten kurtarma amaçlarıyla bu ESHS imza oluşturma ve doğrulama verilerinin kopyalarını yaratır. ESHS imza oluşturma ve doğrulama verilerinin başka bir medyaya yedeklenmesi durumunda bu imza oluşturma ve doğrulama verileri şifrelenmiş formda aktarılır.

Güvenlik sertifikası sahiplerine ait imza oluşturma verileri elektronik imza oluşturma araçlarında oluşturulur

SSL sertifikası sahiplerine ait imza oluşturma verileri başvuru yapan sunucu tarafında oluşturulur ve ancak oluşturuldukları sunucu üzerinde sorunsuz çalışabilir.

6.2.7 Şifreleme Modülünde İmza Oluşturma Verisi Saklanması

Bkz. SUE 6.2.6

6.2.8 İmza Oluşturma Verisinin Aktif Hale Getirilmesinin Metodu

e-Güven ESHS kök sertifikaları imza oluşturma verilerinin aktivasyonu gerekli teknik ve fiziksel güvenlik önlemleri altında sadece birden çok yetkili güvenli personel tarafından gerçekleştirilebilir.

SSL sertifikası sahiplerine ait imza oluşturma verileri SSL sertifikasının imza oluşturma verisi oluşturulan sunucuya yetkili erişim sonrasında yüklenmesi ile aktive olur. İmza Oluşturma Verisinin Aktif Durumdan Çıkarılmasının Metodu
e-Güven ESHS imza oluşturma verisi, imzalama için kullanıldıktan sonra veriye erişim otomatik olarak kesilir.

e-Güven güvenlik sertifikası sahibi imza oluşturma verisinin, elektronik imza oluşturma aracı sistemden çıkartıldığında veya elektronik imza oluşturma aracı sisteme bağlıyken belli bir süre kullanılmadığında veya imzalama işlemi gerçekleştirildikten sonra, etkinliği kaldırılır.

SSL sertifikası sahibi sisteme erişim yapıp sertifikayı aktif yaptıktan sonra sunucu erişilebilir olduğu sürece tanımlanmış olduğu uygulama içinde daima aktif kalır. Herhangi bir zaman aşımı süresi söz konusu değildir. İmza Oluşturma Verisinin Yok Edilmesi Metodu
e-Güven, ESHS imza oluşturma verisinin tam imhasını sağlamak için birden çok ve yetkili güvenli personelin katılımıyla donanım şifreleme modüllerinin sıfırlama işlevinden ve diğer uygun araçlardan yararlanır. Yerine getirilen ESHS imza oluşturma verisi imha faaliyetleri kayıtlara geçirilir.

6.2.9 Şifreleme Modül Operasyonel Limitleri

Koşul yoktur.

6.3 *Anahtar Çifti Yönetiminin Diğer Yönleri*

6.3.1 İmza Doğrulama Verisi Saklanması

e-Güven ESHS sertifikaları ve sertifikalar, e-Güven'in rutin yedekleme prosedürlerinin bir parçası olarak yedeklenir ve arşivlenir.

6.3.2 Sertifikanın Operasyonel Periyodu ve Anahtar Çifti Kullanımı Periyodu

Bir sertifikanın geçerlilik süresi, sertifikanın süresi dolduğunda veya iptal edildiğinde sona erer. İmza oluşturma ve doğrulama verilerinin geçerlilik süresi, ilgili sertifikaların geçerlilik süreleriyle aynıdır, ancak imza doğrulama verileri imza doğrulamak için kullanılmaya devam edilebilir. e-Güven ESHS ve alt kök sertifikalarının geçerlilik süresi 10 yılı geçemez. e-Güven ESHS ve alt kök sertifikalarının geçerlilik süreleri dolmadan önce uygun bir tarihte ilgili ESHS sertifikaları ile imzalanacak yeni sertifikaları düzenlemeyi durdurur.

6.4 *Erişim Verileri*

6.4.1 Erişim Verilerinin Yaratılması ve Kurulması

e-Güven güvenli personelinin erişim verileri, parolaları ve biyometrik verileri içerir. Güvenli personelin parolaları kendileri tarafından yaratılır ve değiştirilebilir niteliğe sahiptir. Biyometrik veriler ise yetkili güvenli personel eşliğinde sisteme kaydedilir.

Sertifika sahibinin erişim verisi ya ESHS tarafından ya da kendisi tarafından yaratılır. Erişim verisinin ESHS tarafından yaratıldığı durumlarda sertifika sahibi derhal erişim verisini değiştirmeli ve kendisinin belirleyeceği erişim verisini yaratmalıdır.

6.4.2 Erişim Verilerinin Korunması

Erişim verilerinin sertifika sahiplerine ve güvenli personele iletilmesinden veya kendileri tarafından yaratılmasından sonra, verilerin gizliliğinin ve güvenliliğinin korunmasıyla ilgili sorumluluk sertifika sahiplerine ve güvenli personele aittir. Güvenli personele iletilmeyen erişim verileri kasalarda ve farklı lokasyonlardaki fiziksel güvenliğe sahip alanlarda saklanırlar.

6.4.3 Erişim Verileriyle İlgili Diğer Durumlar

Koşul yoktur.

6.5 *Bilgisayar Güvenlik Kontrolleri*

6.5.1 Özel Bilgisayar Güvenliği Teknik Gereklilikleri

e-Güven, ESHS yazılımlarının ve veri dosyalarının bakımını yapan sistemlerin yetkisiz erişime karşı korunmuş güvenilir sistemler olmasını sağlar. Ayrıca, e-Güven, üretim sunucularına erişim, bu erişim için geçerli bir faaliyet sebebi olan bireylerle sınırlar. Genel uygulama kullanıcılarının, üretim sunucularında hesapları yoktur.

e-Güven'in üretim ağı diğer bileşenlerden mantıksal olarak ayrılır. Bu ayrım, tanımlanmış başvuru süreçleriyle yapılanlar haricindeki ağ erişimlerini engeller. e-Güven, üretim ağını dahili ve harici izinsiz girişlere karşı korumak ve üretim sistemlerine erişebilecek ağ faaliyetlerinin niteliğini ve kaynağını sınırlamak için güvenlik duvarları kullanır.

6.5.2 Bilgisayar Güvenliği Operasyonel Limitleri

e-Güven'in çekirdek ESHS Güven Merkezi yazılımı ISO/IEC 15408-3:1999 'un EAL 4 seviye gerekliliklerini karşılar.

6.6 *Yaşam Zinciri Teknik Kontrolleri*

6.6.1 Sistem Geliştirme Kontrolleri

e-Güven sistem geliştirme kontrolleri TS ISO/IEC 27001 kontrolleri ve gereksinimleri ortaya çıkan risk kontrolü ve risk azaltma metodları doğrultusunda gerçekleştirilir.

6.6.2 Güvenlik Yönetim Kontrolleri

e-Güven, TS ISO/IEC 27001 kontrolleri doğrultusunda gerekli güvenlik yönetimi kontrollerini gerçekleştirir.

6.6.3 Yaşam Zinciri Teknik Kontrolleri

Koşul yoktur.

6.7 *Ağ Güvenlik Kontrolleri*

e-Güven ağ üzerindeki bütün işlevlerini, yetkisiz erişimlere ve diğer kötü niyetli faaliyetlere karşı koruma amacıyla güvenliği sağlanmış ağlar kullanarak yerine getirir. e-Güven, gizli bilgilerin iletimini şifreleme, dijital imzalar ve güvenli elektronik imzalar kullanarak korur.

6.8 *Zaman Damgası*

Bkz. ZDUE, ZDİ

7. Sertifika, SİL ve Çevrimiçi Sertifika Durum Protokolü Profilleri

7.1 Sertifika Profili

7.1.1 Sürüm Numarası/Numaraları

Güvenlik sertifikaları ITU-TRec X.509V.3 ve RFC 3280 standardına uygundur.

SSL sertifikaları ITU –Trec X509 V.3 ve RFC 3280 standartlarına uygundur.

7.1.2 Sertifika Uzantıları

ESHS sertifikalarında ve sertifikalarda X.509V.3 (2000) da desteklenen bütün uzantılar kullanılabilir.

Güvenlik sertifikalarının anahtar kullanım alanları uzantılarında inkar edilemezlik (non-repudiation) ve dijital imza (digital signature) uzantılarının kullanılmasına izin verilir. ESHS sertifikalarında ise sertifika imzalama (KeyCertSign), SİL imzalama (CRLSign), çevrimdışı SİL imzalama (off-line CRLSign) anahtar kullanım uzantıları kullanılır.
ANAHTAR KULLANIM ALANLARI FARKLI ŞEKİLDE AYARLANABİLMEKTEDİR.

SSL sertifikalarında Key Agreement ve Key encipherment anahtar kullanımları zorunlu olarak kullanılmaktadır. Diğer anahtar kullanımları projeye göre eklenebilmektedir.
Algoritma Nesne Belirteçleri (OID)
Kullanılan algoritmaların nesne belirteçleri sertifika içerisinde belirtilmektedir.

7.1.3 İsim Formları

Sertifikalardaki isim alanları ITU X.500 "Distinguished Name" (Tekil Kayıt Adı) biçimine uygundur.

7.1.4 İsim Kısıtlamaları

Koşul yoktur.

7.1.5 Sertifika İlkeleri Nesne Belirteci

Sertifikalarda bağlı oldukları sertifika ilkelerinin nesne belirteci ve nitelikli elektronik sertifika olduklarına ilişkin nesne belirteçleri yer alır.

7.1.6 Sertifika İlkeleri Kısıtlamaları Uzantısının Kullanımı

Koşul yoktur.

7.1.7 Sertifika İlkeleri Belirteçleri için Yazımsal ve Anlamsal Özellikler

e-Güven alt kök sertifikalarının sertifika ilkeleri uzantıları içerisindeki ilke niteleyicilerde SUE'ye ulaşmak için gerekli bir URL ve "Bu sertifika ile ilgili sertifika uygulama esaslarını okumak için belirtilen dokümanı açınız" şeklinde bir ibare bulunur.

7.1.8 Kritik Sertifika İlkeleri Uzantıları için Anlamsal İşlem Özellikleri

Koşul yoktur.

7.2 *SİL Profili*

7.2.1 Sürüm Numarası/Numaraları

e-Güven X.509 Sürüm 2 CRL (SİL) 'ler yayınlamaktadır.

7.2.2 SİL ve SİL Girdi Ekleri

SİL'lerde RFC 3280 tarafından tanımlanan uzantılar kullanılır.

7.3 *Çevrimiçi Sertifika Durum Protokolü (ÇSDP) Profili*

ÇSDP gerçek zamanlı Sertifika sorgusu hizmetidir.

7.3.1 Sürüm Numarası(Veya Numaraları)

RFC 2560 desteklenmektedir.

7.3.2 ÇSDP Uzantıları

RFC 2560 desteklenmektedir.

8. Uyum Denetimi ve Diğer Değerlendirmeler

e-Güven, TSE tarafından TS ISO/IEC 27001 standardına uyumluluk açısından denetlenir. e-Güven TS ISO/IEC 27001 kontrolleri doğrultusunda ayrıca kendi iç kontrollerini gerçekleştirir.

8.1 *Değerlendirmelerin Sıklığı ve Değerlendirme Durumları*

e-Güven'in kendi inisiyatifi ile yaptığı değerlendirmeler e-Güven PYO tarafından gerekli görüldüğü durumlarda yapılacaktır. TS ISO/IEC 27001 sertifikasına bağlı uyumluluk denetimleri her yıl yapılacaktır.

8.2 *Değerlendirme Yapan Kişinin Tanımlanması Ve Nitelikleri*

TS ISO/IEC 27001 sertifikasına bağlı uyumluluk denetimleri yetkili bir denetçi tarafından yapılacaktır. e-Güven iç denetimleri yetkili güvenli personel tarafından yapılacaktır

8.3 *Değerlendirme Yapan Kişinin Değerlendirme Yapılan Kuruluşla İlişkisi*

Bkz. SUE 8.2

8.4 *Değerlendirme Tarafından Kapsanan Konular*

TSE tarafından TS ISO/IEC 27001 standardına ilişkin yapılan denetimlerde standarda uyumluluk denetlenecektir. e-Güven tarafından yapılan iç denetimlerde TS ISO/IEC 27001 kontrolleri gereği yapılan iç denetimler ve işleyişin SUE'ye uygunluğu denetlenecektir.

8.5 *Eksikliğin Ortaya Çıkması Durumunda Gerçekleştirilecek Eylemler*

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

8.6 *Değerlendirme Sonuçlarının Yayınlanması ve İlgili Taraflara İletimi*

e-Güven tarafından yapılan denetimlerin sonuçları, ilgili e-Güven personeline ve yönetime iletilir.

9. Diğer Ticari Ve Hukuki Konular

9.1 *Ücretler*

9.1.1 Sertifika Yayınlama veya Yenileme Ücretleri

e-Güven, sertifikaların düzenlenmesi, yönetimi ve yenilenmesi için sertifika sahiplerine ücret tahakkuk ettirmeye yetkilidir. Sertifika sahiplerine uygulanan ücretlerle ilgili bilgiye e-Güven'in web sitesinden ulaşılabilir.

9.1.2 Sertifikalara Erişim Ücretleri

e-Güven, bir sertifikanın veritabanından sorgulanması veya başka herhangi bir şekilde üçüncü kişilerin kullanımına sunulması karşılığında herhangi bir ücret tahakkuk ettirmez.

9.1.3 Sertifikaların İptal veya Durum Kayıtlarına İlişkin Bilgilere Erişim Ücretleri

e-Güven, SİL ve ÇSDP hizmetleri için herhangi bir bir ücret tahakkuk ettirmez.

9.1.4 Diğer Hizmetler İçin Ücretler

9.1.4.1 Zaman Damgası Ücretleri

e-Güven zaman damgası hizmetleri için sertifika sahiplerine ücret tahakkuk ettirmeye yetkilidir. Zaman damgası hizmetleri ücretleri ile ilgili ayrıntılı bilgiye e-Güven web sitesinden ulaşılabilir.

9.1.4.2 Sertifika İlkeleri Bilgisi Gibi Diğer Servislerin Ücretleri

e-Güven, sertifika ilkelerine ve SUE'ye erişim için bir ücret tahakkuk ettirmez. Çoğaltma, başkalarına dağıtma, değişiklik veya işleme gibi dokümanın inceleme haricindeki amaçlarla kullanımı, e-Güven'le yapılan lisans anlaşmasına tâbidir.

9.1.5 Geri Ödeme Politikası

Koşul yoktur.

9.2 *Finansal Sorumluluklar*

9.2.1 Sigorta Kapsamı (Sertifika Mali Sorumluluk Sigortası)

SUE kapsamındaki sertifikalar için herhangi bir sigorta uygulanmamaktadır.

9.2.2 Diğer Varlıklar

Koşul yoktur.

9.2.3 Son Kullanıcılar İçin Sigorta veya Diğer Garantilerin Kapsamı

Bkz. SUE 9.2.1

9.3 *Ticari Bilgilerin Gizliliği*

9.3.1 Gizli Bilgilerin Konusu

Sertifika sahiplerine ait aşağıdaki bilgiler gizli bilgi sayılacaktır;

- sertifika başvuru kayıtları
- İşlem kayıtları

e-Güven'e ait aşağıdaki bilgiler gizli bilgi sayılacaktır;

- İş planları
- Kamuya açıklanıncaya kadar denetim ve değerlendirme kayıtları
- Felaketten kurtarma ve olasılık planları
- e-Güven'in ESHS işleyişinde kullandığı donanım ve yazılımla ilgili teknik güvenlik bilgileri ve Güven Merkezi ile ilgili bilgiler

9.3.2 Gizli Bilgilerin Konusu İçerisinde Olmayan Bilgiler

Sertifika içerisinde yer alan bilgiler, sertifika iptali ve diğer durum bilgileri e-Güven bilgi deposunun içindeki bilgiler.

9.3.3 Gizli Bilgilerin Korunmasına İlişkin Sorumluluklar

e-Güven SUE ile gizli bilgi olarak kabul edilen bilgileri gizli olarak tutacak ve yetkili kamu kurumları ve yargı mercilerinin talepleri dışında üçüncü kişilere açıklamayacaktır.

9.4 *Kişisel Bilgilerin Mahremiyeti (Gizliliği)*

9.4.1 Mahremiyet Planı

Koşul yoktur.

9.4.2 Özel Sayılan Bilgiler

Sertifika içeriğinde ve SİL'lerde yer almayan bilgiler özel kişisel bilgilerdir.

9.4.3 Özel Sayılmayan Bilgiler

Sertifikada ve SİL'lerde herkesin erişimine açık bir şekilde yayınlanan bilgiler özel kişisel bilgiler değillerdir.

9.4.4 Gizli Bilginin Korunma Sorumluluğu

Güvenli personel, kendi iştanımları doğrultusunda işbu SUE ve ilgili sözleşmelerde gizli bilgi olarak tanımlanan bilgiyi korumak zorundadır.

9.4.5 Kişisel Bilgilerin Kullanılmasına İlişkin Bildirim ve İzin

e-Güven sertifika sahibinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

9.4.6 Adli ve İdari Süreçlerde Kullanılmak Üzere Yapılan Açıklamalar

Sertifika sahipleri ve ilgili taraflar, e-Güven'in, 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.

9.4.7 Bilgilerin Açıklandığı Diğer Durumlar

Koşul yoktur.

9.5 *Fikri Mülkiyet Hakları*

Fikri mülkiyet haklarının katılımcılar arasında kime ait olduğu e-Güven ile ilgililer arasında yapılan sözleşmelerle belirlenir. Bunun dışında e-Güven tarafından yayınlanan tüm sertifikalar, sertifika iptal bilgileri, SUE, sertifika ilkeleri, kullanıcı sözleşmeleri, e-Güven tarafından hazırlanmış her türlü doküman, veritabanı, web siteleri ve bu web sitelerinde yer alan her türlü metin, görsel ve işitsel içeriğin fikri mülkiyet hakları e-Güven'e aittir.

9.6 *Sorumluluk ve Garantiler*

9.6.1 ESHS'nin Sorumluluk ve Garantileri

e-Güven Sertifika Sahipleri ve üçüncü kişilere ;

- Elektronik Sertifika Hizmet Sağlayıcısı olarak, SUE ile belirlenen yükümlülükleri yerine getirerek faaliyetlerini yürüttüğünü ve/veya yürüteceği
- Sertifikanın oluşturulduğu zamanda içeriğindeki bilgilerin doğru olduğu ve bu bilgilerin SUE'de belirtilen belgelere dayanarak tespit edildiği
- İmza sahibinin sertifikada belirtilen imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olduğu
- Bütün sertifika iptal, askı taleplerini değerlendirdiği ve kaydettiği

Konularında garanti verir.

9.6.2 KM'nin Sorumlulukları ve Garantileri

Koşul yoktur.

9.6.3 Sertifika Sahibinin Sorumlulukları ve Garantileri

Sertifika sahibi, geçerliliği sona ermiş, askıda bulunan veya iptal edilmiş sertifikayı kullanmamakla, kendisine ait olan imza oluşturma verisini kimseye kullandırmamakla, erişim verilerinin gizliliğini sağlamakla, sertifikayı ve buna bağlı imza oluşturma verisini kullandığı ortamların gizliliğini ve güvenliğini sağlamakla, sertifikayı imzalamış olduğu kullanıcı sözleşmesine, SUE'ye, ilgili sertifika ilkelerine uygun olarak ve hukuka uygun amaçlarla kullanmakla, başvuru süreçlerinde e-Güven personeline doğru, geçerli ve yeterli bilgi ve belgeleri sağlamakla yükümlüdür.

Sertifika sahiplerinin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğan veya doğmuş olacak e-Güven'in, üçüncü kişilerin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır.

9.6.4 Üçüncü Kişilerin Sorumlulukları ve Garantileri

Üçüncü Kişiler, sertifikaya güvenerek işlem yapmak için bu sertifikada yer alan bilgilerin doğruluğunu kontrol edebilme hususunda yeterli bilgiye sahip olduklarını, bu bilgileri kullanıp kullanmama konusunda karar vermekten tek başlarına sorumlu olduklarını kabul ederler.

Üçüncü Kişiler sertifikaya güvenerek herhangi bir iş veya işlem yapmadan önce elektronik imzayı doğrulamakla ve sertifikanın geçerliliğini kontrol etmekle yükümlüdürler.

Üçüncü kişilerin, yukarıda belirtilen yükümlülüklerini yerine getirmedikleri takdirde bu yükümlülüklerini yerine getirmemeleri sebebiyle doğmuş ve doğacak e-Güven'in, sertifika sahiplerinin, üçüncü kişilerin ve ilgili diğer tarafların zararlarını tazmin sorumlulukları vardır. ederler.

9.6.5 Diğer Katılımcıların Sorumlulukları ve Garantileri

e-Güven ESHS işleyişini sürdürürken üçüncü taraflarla bazı hizmetlerin gördürülmesini sağlamak üzere hizmet sözleşmeleri yapabilir. Bu noktada anlaşma yapılan üçüncü tarafların hakları, sorumlukları ve yükümlülükleri kendileriyle yapılan ilgili hizmet sözleşmeleri uyarınca belirlenir.

9.7 *Garantilerin Reddi*

Kullanıcı Sözleşmelerinde e-Güven'in garantilerinin reddi ile ilgili hükümler bulunur.

9.8 *Tazminatlar*

Bkz. SUE 9.6

9.9 *SUE'nin Geçerliliği ve Sona ermesi*

9.9.1 Geçerlilik

Bu SUE ve SUE'ye yapılan eklemeler, e-Güven bilgi deposunda yayınlanmasından (geçerlilik süresi ayrıca belirtilmişse bu süreden) itibaren geçerlilik kazanır.

9.9.2 Sona Erme

Bu SUE yeni bir sürüm ile yenilenmesinden itibaren geçerliliğini kaybeder.

9.9.3 Sona Ermenin Etkileri

Bu SUE'nin geçerliliğinin sona ermesinden itibaren katılımcılar bu SUE'nin hükümleri ile bağlı değildir. SUE'nin geçerliliğinin sona ermesinden sonra yürürlüğe giren yeni SUE'nin hükümleri ilgili tüm taraflar için geçerli olacaktır

9.10 *Bireysel Bildirimler ve Katılımcılar Arasında İletişim*

e-Güven ve katılımcılar arasında iletişim e-mail, sms, yazılı ihtar ve çağrı merkezi aracılığıyla yapılacaktır.

9.11 *Değişiklikler*

9.11.1 Değişiklik Prosedürleri

SUE'deki değişiklikler PYO tarafından yapılacaktır. Değişiklikler ya SUE'nin düzeltilmiş halini içeren bir doküman formunda, ya da bir güncelleme şeklinde yapılacaktır. Değişikliğe uğramış

Sürümler veya güncellemeler web sitesinde yayınlanacaktır. Güncellemeler, SUE'nin atıfta bulunulan sürümünün belirtilen veya çelişkili hükümlerini geçersiz kılar.

9.11.2 Bildirim Mekanizması ve Periyodu

e-Güven, SUE içersinde gerçekleştirdiği tek taraflı düzeltmeler ve değişiklikler için önceden ihbarda bulunmadan SUE'de düzeltme ve değişiklik yapma hakkını saklı tutar.

9.11.3 Sertifika İlkeleri Belirteci (OID) veya "SUE" İşaretinde Değişiklik Gerektiren Değişiklikler

Sertifika ilkeleri belirteçlerinde değişiklik gerektiren haller PYO tarafından belirlenecek ve ilgili sertifika ilkeleri dokümanında değişikliğe gidilecektir. Bunun dışında ve genel olarak yapılan eklemeler için sertifika ilkeleri tanımlayıcısında ve SUE işaretinde değişikliğe gidilmez.

9.12 *Uyuşmazlıkların Çözüm Yolları*

İşbu SUE ile ilgili doğacak uyuşmazlıklarda, Tarafların vekilleri Avukatlık Kanunu 35/A Maddesi uyarınca bir araya gelip karşılıklı olarak uzlaşmaya çalışacaktır. Uyuşmazlık konusu olan olay hakkında işbu madde içersinde öngörülen usulle taraflar arasında 1 (Bir) Ay içersinde herhangi bir sonuç alınamaması durumunda Taraflar yargı yoluna gitmekte serbest olacaklardır. İşbu SUE ile ilgili doğacak uyuşmazlıklarda İstanbul Mahkemeleri ve İcra Daireleri yetkilidir.

9.13 *Uygulanacak Hukuk*

İşbu SUE'nin uygulanması, oluşturulması, yorumlanması ve geçerlilik süresi, Türk Hukukuna tabidir.

9.14 *Mevzuata Uyumluluk*

İşbu SUE Türkiye'de geçerli yerel mevzuata uygun olarak hazırlanmıştır.

9.15 *Çeşitli Hükümler*

9.15.1 Bütün sözleşme

Koşul yoktur.

9.15.2 Devir ve Temlik

Koşul yoktur.

9.15.3 Bölünebilirlik

e-Güven Kullanıcı Sözleşmeleri, bölünebilirlik, post-contractus hükümler, bütünlük ve ihbar hükümleri içerir. Bir sözleşmedeki bölünebilirlik hükmü, sözleşmedeki bir maddenin

geçerliliğinin veya uygulanabilirliğinin sona erdiği yönünde yapılan bir tespitin sözleşmenin diğer hükümlerinin de geçersiz olmasını önler. Post – Contractus Hükümler, sözleşmenin feshedilmesine veya sona ermesine rağmen yürürlükte kalacak hükümleri belirtir. Bütünlük hükmü, sözleşmenin konusuyla ilgili tüm mutabakatın sözleşmeye dahil edildiğini belirtir. Bir sözleşmedeki ihbar hükmü, tarafların birbirlerine nasıl ihbarda bulunacağını belirtir.

9.15.4 Yaptırımlar (Vekalet Ücreti ve Haktan Feragat)

Koşul yoktur.

9.15.5 Mücbir Sebep

Cari kanunların ve ilgili mevzuat hükümlerinin izin verdiği sınırlar içerisinde, Kullanıcı Sözleşmelerine mücbir sebep maddesi dahil edilmiştir.

9.16 *Diğer Hükümler*

Koşul yoktur.

EK A - Tanımlar ve Kısaltmalar Tablosu

KAVRAM/KISALTMA	AÇIKLAMA/TANIM
Başvuru Yöntemleri	ESHS ile sertifika başvurusunda bulunan kişi arasında başvurunun yapılması, sertifika sahibinin kimliğinin tespiti, gerekli evrakların hazırlanması, sertifika ücretlerinin ödenmesi, evrakların saklanması, nitelikli elektronik sertifikaların yayınlanması ve sertifika sahibine iletilmesi, sertifika iptal, yenileme ve askı taleplerinin iletimindeki usuller gibi hususların belirlendiği teknik ve idari süreçlerden oluşan yöntemler. Bu yöntemlere ESHS'nin Web adresinden ulaşılabilir.
CEN	Comité Européen de Normalisation - Avrupa Standardizasyon Komitesi
CWA	CEN Workshop Agreement- CEN Çalıştay Kararı
ÇSDP	Çevrimiçi Sertifika Durum Protokolü
EAL	Evaluation Assurance Level - Değerlendirme Garanti Düzeyi
Elektronik İmza Kanunu	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Kanun.
ESHS	Elektronik Sertifika Hizmet Sağlayıcı (e-Güven)
Erişim Verisi	Güvenli elektronik imza oluşturma araçlarına erişim için kullanılan parola, biyometrik değer gibi verileri.
ETSI	European Telecommunication Standartization Institute- Avrupa Telekomünikasyon Standartları Enstitüsü
ETSI TS	ETSI Technical Specifications - ETSI Teknik Özellikleri
GKNESİ	Genel Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
Güvenli Elektronik İmza	Güvenli elektronik imza; Münhasıran imza sahibine bağlı olan, Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, Elle etılmış imzayla aynı hukuki sonuçları doğuran Elektronik imzadır.
Güvenli Elektronik İmza Doğrulama Aracı	Güvenli elektronik imza doğrulama araçları; İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren, İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren, Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan, İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

	İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren, İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan ve CWA 14171 standardına uygun imza doğrulama araçlarıdır.
Güvenli Elektronik İmza Oluşturma Aracı	Güvenli elektronik imza oluşturma araçları; Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini, Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını, 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 araçlardır.
Güvenli Personel	Sertifika yaşam zinciri ve güvenli elektronik imza oluşturma aracı yönetim kontrolleri, anahtar yönetimi kontrolleri, ESHS sertifika yönetim sistemleri ve veri bankaları kontrolleri faaliyetlerini gerçekleştiren, gerekli erişim ve kontrol yetkisine sahip e-Güven veya e-Güven yetkilisi personeli (Bkz. SUE 5.2.1)
IETF RFC	Internet Engineering Task Force Request for Comments - İnternet Mühendisliği Görev Grubu Yorum Talebi
ISO/IEC	International Organisation for Standardisation / International Electrotechnical Commitee - Uluslararası Standardizasyon Teşkilatı / Uluslararası Elektroteknik Komitesi.
Kanun	23 Ocak 2004 tarih 25355 sayılı Resmi Gazete'de yayımlanan 5070 Sayılı Elektronik İmza Kanunu
Kayıt Makamı (KM)	ESHS'ye bağlı olarak faaliyette bulunan, sertifika başvurusunda bulunan kişiler ile kurumsal başvuru sahiplerinin sertifika başvurularını alan ESHS'nin yetkili birimi.
Kimlik Bilgileri	Sertifika Sahibinin Adı-Soyadı, Türkiye Cumhuriyeti Kimlik Numarası, doğum yeri, doğum tarihi ve uyruğu.
MKNESİ	Mobil Kullanıma İlişkin Nitelikli Elektronik Sertifika İlkeleri
Mobil İmza	Mobil terminaller ve GSM ağı kullanılarak yaratılan Güvenli Elektronik İmza
Mobil Operatör	Mobil operatör, elektronik imza uygulamasında aktif operasyonlarda bulunan sujelere; kendi altyapısı üzerinden iş ve işlemlerde bulunma imkanı sağlamaktadır.
NES	Nitelikli Elektronik Sertifika
NESUE	Nitelikli Elektronik Sertifika Uygulama Esasları
NES Sahibi	Adına ESHS tarafından NES düzenlenen gerçek kişi.
Nitelikli Elektronik Sertifika	5070 Sayılı Kanunun 9. Maddesinde içerik olarak; Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 5.

	Maddesinde ise teknik bakımdan özellikleri belirtilen elektronik sertifika.
OID	Object Identifier - Nesne belirteci.
Sertifika	Elektronik sertifika. SUE içerisinde sertfika nitelikli elektronik sertiki dışında kalan elektronik sertifikaları tanımlamak için kullanılmıştır.
Sertifika İlkesi (Sİ)	Sertifikaların belli bir topluluk ve/veya genel güvenlik gereklilikleri olan uygulamalar bakımından kabul edilebilirliğini belirten kurallar bütününe Sertifika İlkeleri denilmektedir. Sertifika İlkeleri, Elektronik Sertifika Hizmet Sağlayıcıları tarafından umuma açıklanan yukarıda belirtilen amaçları karşılamaya yönelik bir belgedir. ESHS tarafından yayınlanan Sİ'ye, Sİ içerisinde belirtilen tüm katılımcılar uymak zorundadır. Sİ, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, ESHS'nin web sitesinden erişilebilir. İşbu doküman içerisinde geçen Nitelikli Elektronik Sertifika İlkeleri tamlaması Sertifika İlkesi tamlaması ile eş anlamlı olarak kullanılmıştır.
SİL	Sertifika İptal Listesi.
SSCD	Secure Signature Creation Device – Güvenli İmza Oluşturma Aracı
Sertifika Uygulama Esasları (SUE)	Sertifika Sahip'leri 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 içersinde güncellenen ve ESHS tarafından umuma yapılan bir açıklamadır. Sertifika Uygulama Esasları, duruma göre zaman zaman yapılabilecek değişiklikleri de dahil olmak üzere, ESHS'nin web sitesinden erişilebilir. İşbu doküman içerisinde geçen Sertifika Uygulama Esasları tamlaması nitelikli elektronik sertifika dışındaki sertifikaları ile eş anlamlı olarak kullanılmaktadır.
Tebliğ	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ
TC	Türkiye Cumhuriyeti
Üçüncü Kişiler	e-Güven tarafından düzenlenmiş sertifikalara dayanarak menfi ve müspet açıdan iş ve işlemlerde bulunan gerçek ve tüzel kişiler.
Yönetmelik	6 Ocak 2005 tarih 25692 sayılı Resmi Gazete'de yayımlanan Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik.

EK B – Güvenlik Sertifikası Başvurusunda İstenen Belgeler

SERTİFİKA İÇİNDE YER ALACAK BİLGİ	DOĞRULAYACAK RESMİ BELGE
Adı – Soyadı	Nüfus Cüzdanı, Pasaport, Sürücü Belgesi, Avukat Kimlik Belgesi (Avukatlar için) Aslı veya Onaylı Suretleri
T.C. Kimlik Numarası	T.C. Kimlik Numrasının yer aldığı Nüfus Cüzdanı Aslı veya Noter Onaylı Sureti veya T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünün web sitesinden (http://tckimlik.nvi.gov.tr/Web/default.aspx) alınmış web sayfası çıktısının NES Sahibi" imzalı nüshası, İlçe nüfus müdürlüklerinden alınan belge aslı (T.C. Kimlik Numarasının yukarıda belirtilen resmi belgeler içerisinde yer almaması halinde)
Doğum Yeri	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri
Doğum Yılı	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri
Uyruğu	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri
Ülke Kodu	----------
Pasaport No/Bilgiler	Pasaport Aslı veya Noter Onaylı Sureti

EK C – SSL Sertifikası Başvurusunda İstenen Belgeler

SERTİFİKA İÇİNDE YER ALACAK BİLGİ	DOĞRULAYACAK RESMİ BELGE
Adı – Soyadı / Firma Unvani	Nüfus Cüzdanı, Pasaport, Sürücü Belgesi, Avukat Kimlik Belgesi (Avukatlar için) Aslı veya Onaylı Suretleri http://www.sanayi.gov.tr/Sirket/UnvanSorgulama.aspx?menuSec=234 http://www.ticaretsicil.gov.tr/ http://sanayi.tobb.org.tr/
T.C. Kimlik Numarası	http://www.tckimlik.nvi.gov.tr
Doğum Yeri	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri
Doğum Yılı	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri
Uyruğu	Nüfus Cüzdanı, Pasaport, Avukat Kimlik Belgesi (Avukatlar için) Sürücü Belgesi Aslı veya Noter Onaylı Suretleri

Ülke Kodu	----------
Pasaport No/Bilgiler	Pasaport Aslı veya Noter Onaylı Sureti
Alan adı / Domain Name	www.name.com veya .com.tr uzantılı alan adları için www.nic.tr gibi kayıtlı whois sunucularından kontrol edilebilir.