TÜRK STANDARDLARI ENSTİTÜSÜ

SSL SERTİFİKA HİZMET SAĞLAYICILARI (SSHS) İÇİN İDARİ VE TEKNİK YETKİLENDİRME PROGRAMI

Sürüm 1.0

01.12.2013

Revizyon Tarihçesi

Sürüm	Tarih	Güncelleme
0.1	30.06.2013	Şablon oluşturuldu.
0.2	01.10.2013	İdari kriterler eklendi.
0.3	01.11.2013	Teknik kriterler eklendi.
1.0	01.12.2013	Güncellenerek 1.0 olarak yayınlandı.

Bu dokümana aşağıdaki web sayfasından erişilebilir:

- Türk Standardları Enstitüsü Resmi web sitesi (TSE) (bilisim.tse.org.tr) ;

İçindekiler

0. Amaç

Bu kriter programı ile ülkemizde herhangi bir yasal düzenlemeye tabi olmayan SSL sertifikaları ticaretine belirli kriterler getirilerek yaşanabilecek ihlal olaylarının en alt seviyelere çekilmesi, sertifika üretimi ve kullanımında güvenliğin ve güvenin arttırılması amaçlanmaktadır. Bu doğrultuda bu dokümanda SSHS ler için SSL sertifika ticaretinde uymaları gereken gerek idari gerekse teknik şartlar belirlenmiştir.

1. Kapsam

Bu kriter programı, ülkemizde SSL sertifikası üreten SSL Sertifika Hizmet Sağlayıcıların işletimlerinde tüzel kişilik olarak yerine getirmeleri gereken idari ve teknik şartları ve ürettikleri SSL sertifikaların uyum sağlaması gereken teknik şartları kapsar.

Bu kuruluşların SSL sertifikaları dışında ürettikleri Nitelikli Elektronik Sertifikalar bu programın kapsamı dışındadır. SSHS ve Nitelikli Elektronik Sertifika şartları gerek 5070 sayılı Elektronik İmza Kanunu gerekse düzenleyici kurum olan Bilgi Teknolojileri ve İletişim Kurumunun SSHS lere yönelik olarak yayınlamış olduğu yönetmelik ve tebliğler ile düzenlenmiştir. (Nesne imzalama sertifikaları ve VPN sertifikaları)

2. Giriş

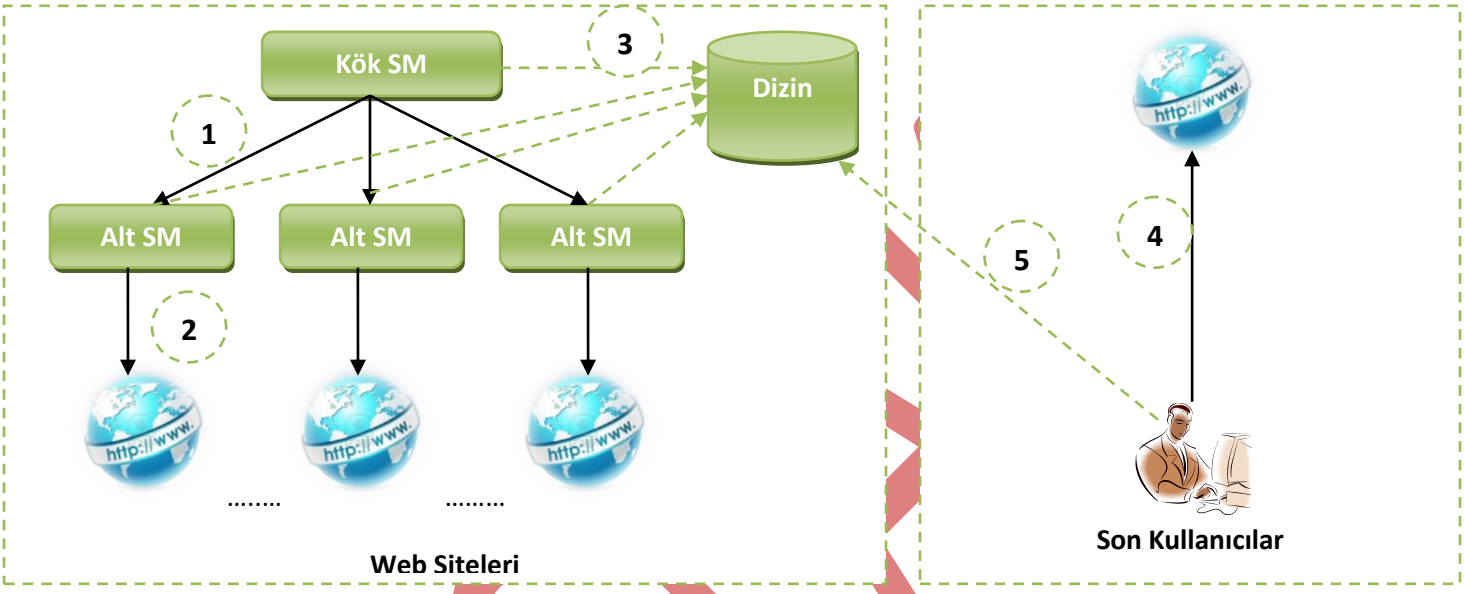
Çevrimiçi iletişim ve veri paylaşımı, verilerin şifrelenmesinde ve sistem ve kişilerin kimliklerinin doğrulanmasında çoğunlukla elektronik sertifikalara dayanır. Elektronik sertifikalar genellikle açık anahtar altyapısı çerçevesinde açık/özel anahtar çiftlerine dayanan kriptografik sistemlerin bütünleşik bir parçasıdır.

HTTPS iletişiminin güvenliği, sunucunun, bazen de istemcinin kimliğinin doğrulanmasına ve aralarındaki iletişimin şifrelenmesine yardımcı olan SSL sertifikalar ile sağlanır. Elektronik sertifikalar aynı zamanda, bir programa güvenip güvenmeme kararı verilirken kaynağının ve doğruluğunun belirlenmesine yardımcı olan yazılım imzalanmasında kritik bir role sahiptirler. Sertifikalar VPN ve Wi-Fi (Kablosuz) bağlantılarının güvenliğini sağlamada da temel oluştururlar.

2.1. Güvenlik ve Güven ilişkisi, Güvenin Sağlanması

Elektronik Sertifika Altyapısının temeli “güven” kavramına dayanmaktadır. Esasen altyapı, bir güven zinciri oluşturulması ve 3. tarafa güvenmeye dayanmaktadır. Bu güven zinciri ve işleyişi şekilde 1 de görülmektedir. Buna göre 1. Adımda Kök Sertifika makamı, Alt sertifika makamlarını sertifikalandırır. Bu şekilde bir güven zincirinin altyapısı oluşmuş olur. 2. Adımda Web siteleri Alt sertifika makamlarına SSL sertifikası almak üzere başvuru yaparlar ve sertifikalandırılırlar. 3. Adımda ise üretilen sertifikalar ve Sertifika iptal listeleri bir dizine

kullanılmak üzere yayınlanırlar. 4. Adımda bir son kullanıcı, web tarayıcısı vasıtasıyla bağlanmak istediği web sitesine https protokolü ile bağlantı isteği gönderir ve 5. Adımda ise web tarayıcısı dizinden sertifika geçerlilik durumu kontrolünü yaparak bağlantıyı tamamlar. Bu işleyiş ile son kullanıcı ile bağlanmak istediği web sitesi arasında bir güven zinciri oluşmuş olur.



Şekil 1: Güven Zinciri ve İşleyişi

Bu noktada bilgi güvenliği ihlal olayları nedeniyle güvenin kaybolması, iş için temel bir risk teşkil etmektedir. Güvenin kaybolmaması için İdari ve teknik şartların belirlenmesi ve idari ve teknik açıdan çeşitli güvenlik kontrollerinin uygulanması gerekmektedir.

2.2. Tehditler ve Riskler ve Sertifikaların Kötü Niyetli Kullanımı

Özellikle son yıllarda, sertifika temelli Açık Anahtar Altyapısının güvenliğinin kırılması ile ilgili bilimsel çalışmalar yapılmakta ve çok yoğun tartışmalar olmaktadır. Bu bölümde sertifikaların tipik kullanımları ve kötü niyetli kullanımları ile ilgili bilgiler verilmektedir.

SSHS lerin işletimine ve temelinde yer alan güven zincirine yönelik olarak çeşitli tehditler ve Risk ler mevcuttur. Özellikle son yıllarda yaşanan SSHS lere yönelik saldırılar, SSHS lerin uluslararası çapta saldırı motivasyonu oluşturduğu gerçeğini ortaya koymaktadır. SSHS lere yönelik en temel ve tehlikeli saldırı tipleri sahte sertifikalar üretilmesi yoluyla web siteleri üzerinden bilgi sızdırılması, ağ iletişiminin dinlenmesi ve SSHS sertifika zincirindeki sertifikaların ele geçirilerek güven zincirinin bozulmasıdır. Aşağıda SSHS lere yönelik bazı temel tehditler ve Riskler bir liste halinde verilmiştir:

2.2.1 Tehditler

Aşağıda yer alan tehditler SSHS işletiminde risk teşkil edebilecek temel tehditleri belirtmektedir :

1. Kök SM sertifikasının ele geçirilmesi
2. Sisteme sızılarak Alt SM sertifikalarının ele geçirilmesi
3. Sisteme sızılarak son kullanıcı sertifikalarının ele geçirilmesi
4. Alt SM lerden sahte sertifika üretilmesi

2.2.2 Riskler

Aşağıda yer alan riskler SSHS işletiminde gerçekleşebilecek temel riskleri belirtmektedir :

1. Çevrimiçi hizmetlerin verilememesi nedeniyle e-imzalama işlemlerinin gerçekleştirilememesi
2. Sahte SSL sertifikaları ile Web sitesi açılarak bilgi sızdırılması ve bu sertifikaların oltalama saldırılarında kullanılması
3. Sahte SSL sertifikalarının ağ cihazlarında (SSL hızlandırıcılar, VPN sunucular vb.) kullanılması ve Ağ iletişiminin dinlenerek bilgi sızdırılması
4. Sahte sertifikalar ile kod parçalarının imzalanarak, kullanıcı bilgisayarlarına kötü niyetli yazılımların yüklenmesi ve bu bilgisayarların zombie haline getirilmesi (Kod imzalama sertifikası)

SSHS sertifika zincirindeki sertifikaların ele geçirilmesi durumunda, SSHS ye ait tüm müşterilerin cihazlarına sahte sertifika üretmek ve bu şekilde örneğin sahte web siteleri hazırlayarak bu web sitelerine kayıt yaptıran kişilerin her türlü gizli ve hassas bilgilerini (Kredi kartı numarası, parolalar, kimlik bilgileri vb.) toplamak mümkündür.

2.2.3 Sertifikaların kötü niyetli kullanımı ve örnekler

Özellikle son yıllarda, elektronik sertifikaların üretildiği ve kullanıldığı Açık Anahtar Altyapısının bazı zafiyetleri ortaya çıkmıştır. Sertifikaların kişilere, kuruluşlara ve kamu kurumlarına saldırılarda kötü niyetli kullanımları görülmüştür.

Çalınan kod imzalama sertifikaları ve bağlı özel anahtarlar kötücül yazılımları imzalamakta kullanılmıştır. Örneğin; bir güvenlik firmasındaki ihlal olayı, şirketin sertifikalarından birinin çalınması ve bu sertifika ile kötü niyetli yazılımların dağıtılmasına sebep olmuştur. Çalındığı açık olan bir sertifika kötücül bir java appletinin imzalanmasında kullanılmıştır. Tarayıcı firması olan Opera'ya yapılan saldırı, saldırganın bir kod imzalama sertifikasına erişmesine ve kötücül yazılım imzalamasına izin vermiştir. Büyük bir grafik ve medya yazılım firmasından çalınan kod

imzalama sertifikaları da kötücül yazılım imzalamada kullanılmıştır. Kurbanların kod imzalama ve diğer sertifikalarını ele geçirmek için kötücül yazılımların geliştirilmesi olağan bir durumdur, bu da kötü niyetli olarak kullanılacak olan çalıntı sertifika olayları ile ilerde daha sık karşılaşacağımız anlamına gelmektedir.

SSHS ler, daha sonradan saldırılarda kullanılacak olan zayıf veya doğru olmayan sertifikalar üretmiştir. Örneğin, bir SSHS bir şirkete yanlışlıkla üretilen bir sertifika satmış ve bu sertifika kötücül çalıştırılabilir bir program imzalamada kullanılmıştır. Bir başka SSHS, zayıf nitelikte "512-bit RSA anahtarlara sahip, sertifika uzantıları olmayan" sertifikalar üretmiştir ve bu sertifikalardan iki tanesi daha sonra diğer bir asyalı sertifika makamına oltalama saldırısı yapan kötü niyetli yazılımın imzalanmasında kullanılmıştır. Bir başka olayda bir SSHS, yanlışlıkla Google'ın sunucularının taklit edilmesini sağlayan bir sertifika üretmiştir ve olay Google tarafından fark edilmiştir.

Aradaki adam saldırıları (MITM), SSL/TLS trafiğini dinlemek amacıyla sertifikaları kötüye kullanmıştır. Yazılımlar, bir sunucunun SSL/TLS sertifikası güvenli fakat sık karşılaşılmayan bir SM tarafından imzalanmışsa nadiren bunu belirtirler veya uyarırlar. Örneğin, bir kişi yaygın kullanılan bir e-posta hizmetine IMAP/SSL ile bağlanırken, sunucu sertifikasının hizmet sağlayıcı tarafından değil farklı bir kuruluş tarafından imzalandığını fark etmiştir. Benzer bir teknik, bir telefon üreticisi firma tarafından, kanuna uygun amaçlarla, telefonların HTTPS iletişimlerinin şifresini çözmek için kullanılmıştır. Muhtemelen, trafiğin meşru olmayan şekilde dinlendiği daha fazla MITM örnekleri de mevcuttur ve ne yazık ki bunların tespit edilmesi de oldukça zordur.

Kötü niyetli yazılımlar, meşru olmayan sertifikalar yükleyerek, bulaştıkları sistemleri kendilerine güvenmek üzere konfigüre etmişlerdir. Örneğin, kötü niyetli bir BHO (Browser Helper Object) sisteme bulaştıktan sonra güvenlik uyarılarını kaldırmak için bilindik bir sertifika makamının sahte sertifikasını güvenilen kök sertifika makamı şeklinde yüklemiştir. Diğer bir örnekte, bir casus yazılım bir yerel SSL/TLS vekil sunucu gibi davranmış ve bu davranışı saklamak için sahte bir sertifika yüklemiştir. Ele geçirilmiş bir sisteme, sahte bir Kök Sertifika Makamı sertifikası yüklemek, aynı zamanda oltalama saldırıları yapmakta da yardımcı olmaktadır. Bunun nedeni ise, saldırganlara SSL/TLS kullanan sahte bir domain oluşturmalarını sağlayarak, sertifika geçerleme adımlarını geçmelerini sağlamalarıdır.

Yukarıda bahsedilenler sadece bazı elektronik sertifikaların kötü niyetli kullanıldığı gerçek hayatta yaşanan bilgi güvenliği ihlal olaylarıdır.

2. Atıf yapılan standartlar ve/veya dokümanlar

Standart	Adı (İngilizce)	TS No	Adı (Türkçe)
CWA 14167-1		Yok	
ETSI 101 456	Electronic Signatures and Infrastructures (ESI) Policy requirements for Certification	Yok	Nitelikli Elektronik Sertifika üreten Sertifika Makamları

	Authorities issuing qualified certificates		için Elektronik imza ve altyapıları politika şartları
ISO/IEC 27001	Information technology – Security techniques – Information security management systems - Requirements	TS ISO/IEC 27001	Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler

3. Terimler ve tarifler

Bu kriter için aşağıdaki terim ve tarifler geçerlidir.

SSHS : 5070 sayılı kanun ile BTK tarafından yetkilendirilmiş olan kuruluşlar.
SSHS : SSL Sertifika Hizmetleri sağlayan ve bu program kapsamında TSE tarafından yetkilendirilmiş olan kuruluşlar.
SM : Sertifikasyon Makamı (TSE tarafından yetkilendirilmemiş)
KM : Kayıt Makamı
SSL : Güvenlik Soket Katmanı
KÖK SM : Güven zincirinde en üstte bulunan Sertifikasyon Makamı
ALT SM : Kök SM tarafından yetkilendirilen Alt Sertifikasyon Makamı
HTTPS : Güvenli http bağlantı
Ağ Adli Bilişimi: Ağ üzerindeki iletişim faaliyetlerinin analiz ve takip edilmesini konu alan Bilişim güvenliği dalı
GSSL SSL : Güvenli SSL sertifikası

4. Kısaltmalar

SSHS : Elektronik Sertifika Hizmet Sağlayıcısı
SSHS : SSL Sertifika Hizmet Sağlayıcısı
SSL : Secure Socket Layers
DNS : Domain Name System
FTP : File Transfer Protocol
HTTP : Hyper Text Transfer Protocol
HTTPS : Hyper Text Transfer Protocol Secure
IP : Internet Protocol
ISO : International Organization for Standardization
TSE : Türk Standartları Enstitüsü
TCP/IP : Transmission Control Protocol/Internet Protocol
UDP : User Datagram Protocol
OWASP : Open Web Application Security Project
Sİ : Sertifika İlkeleri
SUE : Sertifika Uygulama Esasları
SM : Sertifikasyon Makamı

5. SSL Sertifika Hizmet Sağlayıcıları kuruluş yetkinlik şartları

SSHS lerin kuruluş olarak sağlamaları gereken şartlar bu bölümde belirtilmiştir.

5.1. Güvenlik yönetimi şartları

SSHS ler asgari olarak bir Bilgi Güvenliği Politikasına ve SSL sertifikalar ile ilgili olarak bir Sİ (Sertifika İlkeleri) ve SUE (Sertifika Uygulama Esasları) dokümanına sahip olmalıdırlar. Ayrıca SSHS ler işletimlerine yönelik tehditleri ve tehlikeleri de Risk Yönetimi kapsamında ele almalıdırlar. Bilgi Güvenliği Politikası ve Risk Yönetimi, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi çerçevesinde yapılmalıdır.

5.1.1 Sİ

SSHS ler, Sertifika İlkelerinde RFC 3647 ve RFC 2527 de yer alan başlıklar çerçevesinde ve bunlarla sınırlı kalmamak üzere iş uygulamalarını açıklar.

5.1.2 SUE

SSHS ler, Sertifika Uygulama Esaslarında RFC 3647 ve RFC 2527 de yer alan başlıklar çerçevesinde ve bunlarla sınırlı kalmamak üzere iş uygulamalarını açıklar.

5.2. Eğitim şartları

Kurumsal olarak alınması ve tekrarlanması gereken eğitimler ile ilgili olarak Madde 5.5.3 e bakılmalıdır.

5.3. Dokümantasyon şartları

SSHS ler ISO/IEC 27001:2013 ün gerektirdiği doküman şartlarını sağlamalıdır.

5.4. Gizlilik ve kayıt saklama şartları

SSHS'lere ait kurumsal bilgiler,(özellikle Kök SM ve SM özel anahtarları), müşterilere ait tüm bilgiler (özellikle müşteri TC Kimlik No ları, adres telefon vb. bilgiler) ISO/IEC 27001 standardı çerçevesinde uygun güvenlik kontrolleri uygulanarak hassasiyetle saklanmalıdır. Müşteri bilgileri, SSHS ile müşterinin ticari ilişkisinin sonlandığı tarihten itibaren en az 5 yıl süre ile muhafaza edilmelidir.

5.5. Personel şartları

SSHS ler, SSL sertifikaların üretimi, yönetimi ve teknik desteğinin sağlanması ve bu hizmetleri sağlamada gerekli olan diğer altyapı hizmetlerini sağlıklı biçimde yürütebilmek için yeterli teknik bilgiye sahip personel (çalışan veya dış kaynak olarak) istihdam etmelidirler.

5.5.1. Genel şartlar

SSHS lerde teknik olarak en az olmak üzere aşağıdaki rollerde çalışan personel bulunmalıdır:

- Ağ ve Sistem Uzmanı
- AAA Uzmanı
- Bilgi Güvenliği Uzmanı

SSHS'ler Madde 5.5 de belirtilen hizmetleri sağlamak üzere en az olmak kaydıyla 1 kişi ağ ve sistem uzmanı ve 2 kişi güvenlik uzmanı çalıştırmalıdırlar. Güvenlik ile ilgili uzmanlıklar aşağıdaki konuları kapsayacak şekilde ele alınmalıdır;

- Açık Anahtar Altyapısı
- SSL sertifika üretimi ve yönetimi
- Bilgi Güvenliği yönetim sistemi
- Ağ ve sistem güvenliği (Ağ adli bilişimi de dahil olmak üzere)

Yukarıda belirtilen konular 2 veya daha fazla personel istihdam etmek suretiyle kapsanabilir. Ağ ve sistem hizmetleri dış kaynak yoluyla temin edilebilmekle birlikte, güvenlik uzmanları firma bünyesinde genel sağlık sigortalı olarak çalıştırılmalıdır.

5.5.2. Teknik şartlar

SSHS'ler, SM işleyişinin güvenilirliğini destekleyecek ve arttıracak personel ve çalışma uygulamalarını sağlayacak kontrolleri gerçekleştirmelidirler.

Güvenlik rolleri ve sorumlulukları kuruluşun güvenlik politikasında belirlenmeli ve görev tanımları şeklinde yazılı hale getirilmelidir.

SM işletiminin güvenliğinin dayandığı güvenilen roller, açık bir şekilde tanımlanmalıdır. Güvenilen roller asgari olarak aşağıdaki sorumluluklara sahip olmalıdırlar:

a) SSHS güvenlik uygulamalarının gerçekleştirilmesine dair genel sorumluluk;
b) SSL sertifikalarının üretimi, iptali ve askıya alınmasına dair onay;
c) SM sistemlerinin kurulumu, konfigürasyonu ve bakımı ;
d) SM sistemlerinin günlük işletimleri ve sistem yedekleme ve kurtarma;
e) SM sistem arşivleri ve işlem kayıtlarının görülmesi ve bakımı;
f) Kriptografik anahtar yaşam çevirimi fonksiyonları ve
g) SM sistem geliştirme.

5.5.3. Eğitim şartları

SSL sertifika hizmetlerini sağlamada görevli personel belirli aralıklarla eğitime tabi tutulmalıdır. Bu personeller aşağıdaki eğitimleri almalıdır;

1. Bilgi Güvenliği Yönetim Sistemi temel eğitimi
2. Açık Anahtar Altyapısı ve SSL sertifikaları temel eğitimi
3. SSHS işletme süreçleri ve iş akışları

Yukarıda tanımlanan eğitimlerin en az yıllık periyotlarla ilgili personel tarafından alınması sağlanmalıdır.

5.5.3. Güvenlik şartları

SSHS politika ve prosedürleri güvenli roller ve güvenli olmayan roller için adli sicil kaydı ve özgeçmiş doğrulama kontrolleri belirlemelidir. Asgari olarak, güvenli rollerdeki sürekli çalışanlar için, işe kabul öncesinde ve 6 ayda bir olmak üzere doğrulama yapılmalıdır.
Bir çalışanın güvenli olma durumu sistem ve tesislere erişiminden önce veya güvenli durum gerektiren işlemler yapmadan önce onaylanmalıdır.
SSHS çalışanları ve güvenli roller, çalışma şartı olarak bir gizlilik anlaşması imzalamalıdırlar.
Güvenli rollerde çalışan sözleşmeli çalışanlar, en az olmak üzere sürekli çalışan personeller ile aynı geçmiş taramaları ve personel yönetim prosedürlerine tabi olmalıdır.

Alt yükleniciler ve SM ler arasındaki geçici sözleşmeli personel çalıştırılmasına imkan veren tüm sözleşmeler, kuruluşun güvenlik politikalarını ihlal eden sözleşmeli personele karşı tedbirlerin alınmasına açıkça izin vermelidir. Koruma tedbirleri aşağıdakileri içerebilir:

a) Sözleşmeli çalışan personel için bağlayıcılık şartları;

Anahtar yönetimi ve sertifika yönetimi faaliyetlerinde görev alan personelin güvenilirliğinin devam ettiğini doğrulamak için periyodik olarak gözden geçirme yapılmalıdır.

Kuruluşun güvenlik politikalarını ve prosedürlerini ihlal eden çalışanlar için resmi bir disiplin süreci olmalı ve bu uygulanmalıdır. SM'nin politikaları ve prosedürleri, personelin yetkisiz faaliyetlerine, yetkisiz yetki kullanımına ve sistemlerin yetkisiz kullanımına karşı yaptırımları belirtmelidir.

İş akdinin sonlandırılmasını müteakiben çalışanın SM tesislerine fiziksel ve mantıksal erişimi iptal edilmelidir.
Kuruluşun tüm çalışanları ve uygun olan durumlarda 3.taraf altyükleniciler kurumsal politika ve prosedürler hakkında uygun eğitimleri almalıdırlar. SSHS'sının politika ve prosedürleri aşağıdakileri belirtmelidir:

a) Her bir rol için eğitim şartları ve eğitim prosedürleri ve
b) Her bir rol için tekrar eğitim aralığı ve tekrar eğitim prosedürleri.

5.6 İhlal olayı yönetim ve bildirim şartları

SSHS'nin bir bilgi güvenliği ihlal olayı meydana geldiğinde ve özellikle SSL sertifika üretimi zincirinde yer alan Sertifika Makamı sertifikalarının ele geçirilmesi veya bu durumdan şüphe edilmesi durumunda uygulayacakları bir ihlal olayı yönetim prosedürü hazır olmalıdır. Bu prosedürde bu gibi durumlarda ne şekilde hareket edileceği ayrıntısı ile belirlenmelidir. Bu gibi durumlarda asgari olarak;

- Müşterilere ve kamuoyuna olayın kurumsal web sitesi ve/veya e-posta yoluyla duyurulması ve olayın niteliği ile ilgili asgari olarak aşağıdaki bilgilerin verilmesi
    - Olayın gerçekleşme tarihi ve zamanı
    - Şüphelenilen veya tespit edilen Saldırgan
    - Hasar gören veya çalınan bilgiler
    - Olaydan etkilenen müşteri kitlesi veya taraflar
    - Alınan güvenlik tedbirleri

- Alınan tedbirler ve yapılan işlemler hakkında bilgi verilmesi
- TSE ye konu ile ilgili detaylı bilgi verilmesi

İşlemleri gerçekleştirilmelidir.

Ayrıca SSHS'lere bir SOME (Siber olaylara Müdahale Ekibi) kurmaları da tavsiye edilir.

5.7. Yetkilendirme ve iptali

Bu program kapsamında TSE yıllık olarak denetim ve belgelendirme faaliyetlerini yürütür. Denetimden başarıyla geçen firmalara SSHS faaliyet belgesi verilir. Bu denetimlerde majör uygunsuzluk bulunması halinde, uygunsuzluğun en geç 30 iş günü içinde giderilmesi gerekmektedir. Uygunsuzluğun giderilmesini müteakiben TSE tarafından sadece uygunsuzluğa yönelik tekrar denetim yapılır. Minör uygunsuzluk bulunması halinde ise SSHS uygunsuzluğu kapatarak 30 iş günü içerisinde TSE'ye resmi olarak bildirimde bulunur. Her iki durumda uygunsuzlukların giderilmemesi halinde ise TSE belgelendirme komisyonunun kararı ile firma yetki belgesi iptal edilebilir.

5.8 Kapanış işlemleri

SSHS yasal olarak faaliyetlerine son verecek olması durumunda, müşterilerini web sitesinde duyuru yaparak veya e-posta ile en geç 1 ay öncesinden bilgilendirmelidir.

5.9 Yurtdışı hizmet sağlayıcıları

Yurtdışı hizmet sağlayıcıların bu program kriterlerine uyum sağlamayı talep ettikleri durumlarda, kendi adlarına veya yerel iş ortakları üzerinden T.C. kanunlarına tabi resmi tüzel kişilik çatısı altında bu program şartlarını sağlamaları gerekmektedir.

5.10 ISO/IEC 27001 şartları

SSHS ler ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin şartlarına uymak ve uyumluluklarını belgelendirmek zorundadırlar.

6. SSHS teknik şartları

6.1 Açık Anahtar Altyapısının (AAA) önemi

AAA başka bir bireyin veya kuruluşun açık anahtarının gerçekten o bireye/kuruluşa ait olduğunu bilmek için güvenilen taraflara (anlamı, sertifikalar kullanılarak onaylanmış sertifikalara ve/veya dijital imzalara güvende hareket eden sertifikaların alıcıları) bir olanak sağlar. SSHS organizasyonları ve/veya SSHS işlevleri bu ihtiyacı karşılamak için kurulmuştur.
Kriptografi güvenli e-ticaret kurulumu için kritik öneme sahiptir. Bununla birlikte, kriptografi kapsamlı bir güvenlik çözümü sağlamak için diğer güvenli protokoller ile eşleştirilmek zorundadır. Çeşitli kriptografi protokolleri yetkilendirme işlemi için bağımsız bir güvenilir üçüncü taraf (SSHS) tarafından yayımlanan dijital sertifikalara(yürürlülükte olan elektronik yeterlilik belgelerine) gereksinim duyar. SSHS'ları güvenli e-ticarette giderek önemli bir rol üstlenmektedir. Kriptografi'nin kullanımı için mevcut ulusal, uluslararası ve tescilli standartları ve yönergeleri, dijital sertifikaların yönetimi ve SSHS'ların politikaları ve uygulamaları büyük bir bölüm oluşturmasına rağmen bu standartlar düzgün olarak uygulanmamıştır veya yerine getirilmemiştir.

6.2 SSL Sertifika Hizmet Sağlayıcısı

Bu teknolojiler için tarafların güvenli e-ticaret yapmayı etkinleştirmesi, önemli bir sorunun yanıtlanmasını gerektirir. Dijital dünyada bireyin açık anahtarının gerçekten o bireye ait olduğunu nasıl bileceğiz? Yanıtı, bir bireyin açık anahtarı hakkında bilgi içeren elektronik belge olan bir sayısal sertifikadır. Bu belge bir SSL Sertifika Hizmet Sağlayıcısı (SSHS) olarak temsil edilen güvenilir bir organizasyon tarafından dijital olarak imzalanır. Bireyin kimliği ve kendi açık anahtarı arasındaki bağlantı için kefil olan SSHS temel dayanaktır. SSL Sertifika Hizmet Sağlayıcısı, sertifikada bulunan açık anahtarın gerçekten sertifikada belirtilen kuruluşa ait olduğuna dair bir güvence düzeyi sağlar. SSHS tarafından açık anahtar sertifikasına yerleştirilmiş dijital imza, sertifikadaki kuruluşun açık anahtarı, kuruluşun ismi, ve diğer bilgileri örneğin bir geçerlilik süresi, arasında kriptografik bağlantı sağlar. Güvenilen bir tarafın, sertifikanın kurallara uygun bir SSHS tarafından yayımlanıp yayımlanmadığını belirlemesi için, güvenilen taraf yayımlanan sertifikadaki SSHS'nın imzasını doğrulanmak zorundadır. Birçok yaygın Kök SSHS'larının açık anahtarları(sonra tanımlanacak) standart Web tarayıcı yazılımı (örneğin, Mozilla Firefox, Google Chrome veya Microsoft Internet Explorer) içerisine önceden yüklenir. Bu güvenilen tarafa sertifikanın güvenilir bir SSHS tarafından yayımlanıp yayımlanmadığını belirlemesine ve SSHS'nın açık anahtarını kullanarak yayımlanan SSHS'nın imzasını doğrulamasına izin verir.
Bir SSHS'nın amacı sertifikaların üretimini ve yayımlanmasını, dağıtımını, yenilenmesini ve tekrar anahtar üretilmesini, yürürlülükten kaldırılmasını ve askıya alınmasını içeren sertifika yaşam döngüsünü yönetmektir. SSHS, SSHS için temsilciler olarak hareket eden Kök

SSHS'larına müşterilerin ilk kayıt işlemleri için sık sık delege atar. Bazı durumlarda, SSHS kayıt işlemlerini doğrudan icra edebilir. SSHS ayrıca, Sertifika İptal Listesinin(SİL) yayımlanmasına ve/veya aktif durum kontrol mekanizmasının bakımına karşın sertifika durum bilgisinin sağlanması için sorumludur. Genel anlamda, SSHS sertifikaları ve güvenilen taraflarca erişilebilir bir veri havuzu(örneğin çevrim içi bir liste) için yayımlayan SİL leri ilan eder.

6.3 Kayıt Makamı

Kayıt Makamı (KM) kullanıcıların tanımlanması ve yetkilendirilmesinden sorumlu bir kuruluştur, ancak sertifikaları yayımlamaz ya da imzalamaz. Bazı durumlarda, SSHS müşterinin kayıt işlevini dahili olarak icra eder. SSHS diğer durumlarda SSHS olarak aynı yasal kuruluşun bir parçası olacak veya olmayacak harici kayıt otoriteleri(bazen Yerel Kayıt Makamı veya YKM lar olarak adlandırılan) için KM işlevine delege atayabilir. Hali hazırda başka durumlarda, SSHS'nın bir müşterisi(örneğin, bir şirket) KM işlevini SSHS kendisi veya kendi temsilcisini kullanarak gerçekleştirilmesi ile düzenleyebilir.

6.4 Sertifika Uygulama Esasları ve Sertifika İlkeleri

Sertifika Uygulama Esasları (SUE) bir SSL Sertifika Hizmet Sağlayıcısının sertifikaların yayımlanmasında ve yönetilmesinde istihdam etmesi uygulamalarının bir esasıdır. Sertifika İlkeleri(Sİ) yaygın güvenlik gereksinimleri ile belirli bir topluluk ve/veya uygulama sınıfına bir sertifikanın uygulanabilirliğini gösteren adlandırılmış kurallar kümesidir. Örneğin, belirli bir SSL Sertifika Hizmet Sağlayıcısı belirli bir fiyat aralığında eşya ticareti için elektronik veri değişim işlemlerinin doğruluğunun kanıtlanması için bir sertifika türünün uygulanabilirliğini gösterebilir.

6.5 SSL Sertifika Hizmet Sağlayıcıları için ilkeler ve kriterler

Üst düzey kullanıcıya anlaşılır olmak için – müşteri ve güvenilen taraf, aşağıdaki bölümde belirtilen ilkeler güvenilen taraf zihni ile geliştirilmiştir ve, sonuç olarak, dünyada uygulamalı ve teknik olmayan olması için amaçlanır.

6.5.1 SSL Sertifika Hizmet Sağlayıcısı İlkeleri

6.5.1.1 SSHS iş uygulamalarının açıklanması

SSL Sertifika Hizmet Sağlayıcısı:

- Sertifika Uygulama Esaslarındaki İşini, Anahtar Yaşam Döngüsü Yönetimini, Sertifika Yaşam Döngüsü Yönetimini ve SSHS çevresel kontrol uygulamalarını açıklar ve
- Sertifika İlkelerindeki(mevcut ise) İşini, Anahtar Yaşam Döngüsü Yönetimini, Sertifika Yaşam Döngüsü Yönetimini ve SSHS çevresel kontrol politikalarını açıklar.

SSL Sertifika Hizmet Sağlayıcısı aşağıdaki maddelerin güvencesini sağlamak için etkin kontrollerini uygular:

- SSHS'nın Sertifika Uygulama Esasları kendi Sertifika İlkeleri(mevcut ise) ile tutarlıdır ve
- SSHS kendi Sertifika İlkelerine (mevcut ise) uygun olarak hizmetlerini sağlar.

SSHS anahtarını ve sertifika yaşam döngüsü yönetimi işini ve bilgi gizliliği uygulamalarını ifşa etmek zorundadır. SSHS nın iş ile ilgili bilgileri tüm müşterilere ve genel anlamda Web sayfası üzerinde iletilen tüm potansiyel güvenilen taraflara ulaşılabilir olmalıdır. Bu tür ifşa bir Sertifika İlkelerinde (Sİ) ve/veya Sertifika Uygulama Esaslarında (SUE), veya kullanıcılarca(müşteriler ve güvenilen taraflar) ulaşılabilir diğer bilgilendirici materyaller içerisinde yer alabilir.

6.5.1.2 Hizmet bütünlüğü

SSL Sertifika Hizmet Sağlayıcısı aşağıdaki maddelerin güvencesini sağlamak için etkin kontrollerini uygular:

- Anahtarların ve sertifikaların bütünlüğünün tesis edilmesi ve onların yaşam döngüleri boyunca korunması;
- Müşteri bilgisinin düzenli olarak doğrulanması (SSHS lertarafından gerçekleştirilmiş kayıt faaliyetleri için); ve
- Alt SM sertifika isteklerinin doğru, doğrulanmış ve onaylanmış olması.

Etkili anahtar yönetim kontrolleri ve uygulamaları açık anahtar altyapısı güvenilirliği için çok önemlidir. Anahtar şifreleme yönetim kontrolleri ve uygulamaları SSHS anahtar üretimini, SSHS anahtar saklamasını, yedeklemesini ve kurtarmasını, SSHS açık anahtarı dağıtımını(özellikle kendi kendine imzalana kök sertifikaların formunda yapıldığında), SSHS anahtarı üçüncü şahsa verilmesini(mevcut ise), SSHS anahtar kullanımını, SSHS anahtar imhasını, SSHS anahtar arşivlemesini, kendi yaşam döngüsü boyunca SSHS şifreleme donanımının yönetimini ve SSHS tarafından sağlanmış müşteri anahtar yönetim hizmetini(mevcut ise) kapsar ve güçlü anahtar yaşam döngüsü yönetim kontrolleri açık anahtar altyapısının bütünlüğüne zarar verebilir olan anahtar uzlaşmasına karşı korumak için çok güçlüdür.

Kullanıcı sertifikası yaşam döngüsü SSHS tarafından sağlanan hizmetlerin odağındadır. SSHS kendi yayınladığı SUE ve Sertifika İlkelerinde sunacağı hizmetler ile kendi standartlarını ve uygulamalarını oluşturur. Kullanıcı sertifika yaşam döngüsü aşağıdaki maddeleri içerir:

- Kayıt (anlamı, sertifika için bireysel müşteri bağlanması ile ilgili tanımlama ve doğrulama süreci);
- Sertifikaların yenilenmesi(mevcut ise);
- Sertifikaların anahtar yenilemesi;
- Sertifikaların yürürlülükten kaldırılması;
- Sertifikaların askıya alınması(mevcut ise) ;
- Sertifika durum bilgilerinin güncel olarak açıklanması(Sertifika İptal Listeleri veya çevrimiçi sertifika durum protokolünün bazı biçimleri); ve
- Yaşam döngüleri boyunca(mevcut ise) gizli anahtarları taşıyan tümleşik devre kartlarının(ICC) yönetimi.

Zayıf tanımlama ve doğrulama kontrolleri SSHS tarafından yayımlanan sertifikalara güvenen müşterilerin ve güvenilen tarafların becerilerini tehlikeye atacağından, kayıt süreci üzerinde etkin kontroller çok önemlidir. SSHS tarafından yayımlanmış sertifikalara güvenilemediğini bilmek müşteriler ve güvenilen taraflar için kritik olduğu gibi, etkin yürürlükten kaldırma prosedürleri ve sertifika durum bilgilerinin güncel olarak açıklanması da kritik unsurdur.

6.5.1.3 SSHS çevresel kontrolleri

SSL Sertifika Hizmet Sağlayıcısı aşağıdaki maddelerin güvencesini sağlamak için etkin kontrollerini uygular:

- Yetkili kişilerle sınırlandırılmış SSHS sistemlerine ve verilerine mantıksal ve fiziksel erişimi;
- Anahtarın devamlılığı ve sertifika yönetim işlemlerinin sürdürmesi ve
- SSHS sistemleri gelişmesi, bakımı ve SSHS sistem bütünlüğünün devam ettirmek için işlemlerin düzgünce yetkilendirilmesi ve gerçekleştirilmesi.

Güvenilir bir SSHS çevresinin kurulması ve sürdürülmesi, SSHS'nın iş sürecinin güvenilirliği için çok önemlidir. Güçlü SSHS çevresel kontrolleri olmadan, güçlü anahtar ve sertifika yaşam döngüsü kontrolleri ciddi değer kaybeder. SSHS çevresel kontrolleri SUE ve Sİ yönetimini, güvenlik politikası yönetimini, güvenlik yönetimini, varlık sınıflandırması ve yönetimini, çalışan güvenliğini, SSHS faaliyetlerinin fiziksel ve çevresel güvenliğini, işlemler yönetimini, sistem erişim yönetimini, sistem geliştirmesi ve sürdürülmesini, iş devamlılığı yönetimini, izleme ve uygunluğunu ve olay günlüğü tutmayı içerir.

7. SSL sertifikaları teknik şartları

SSL sertifikaları çevrimiçi olarak iletilen bilgileri, üçüncü taraflar tarafından dinlenme ve çalınmaya karşı şifreler ve korur. SSL sertifikaları teknoloji olarak standart olmakla beraber, sertifika üretiminde yürütülen idari süreçler (kimlik doğrulama ve diğer süreçler) bakımından Standart ve Güvenli SSL sertifikaları olarak ikiye ayrılır.

7.1. Standart ve Güvenli SSL Sertifikaları

Standart SSL sertifikaları, bir SSHS tarafından, bir web sitesi için sertifika üretilirken kimlik doğrulama aşamasında yüksek güvenlik seviyesine sahip olunmadan üretilen SSL sertifikalarıdır. Standart SSL sertifikaları, kullanıcılara bir web sitesinin kimliğini çapraz kontrol yapmalarına imkân vermez.
Standart SSL sertifikaları aynı zamanda "Domain-validated" (DV) SSL sertifikaları olarak da adlandırılırlar. Bu tür sertifikaları çevrimiçi olarak bir insan tarafından herhangi bir kimlik doğrulaması yapılmadan almak kolaydır. Özellikle Standart SSL sertifikaların alınmasındaki kolaylık, oltalama yapanları ve diğer kötü niyetli kişileri çevrimiçi saygınlıklarını tesis etmede cesaretlendirmiştir.

Bir SSHS, sertifikaların üretildiği varlığın kimliğini doğrulamak için ek adımlar uyguladığı durumda, üretilen sertifikalar standart sertifikalardan farklı hale gelerek Güvenli SSL (“GSSL”) sertifikaları adını alır. Bu sertifikaların verilmesi aşamasında hem domain hem de firma kimlik doğrulaması yapıldığından dolayı, bu sertifikalar Web sitesine ve sahibinin kimliğine dair daha fazla güvence sağlar.

“Güvenli SSL” (GSSL) sertifikaları mevcut SSL sertifika formatı üzerine bina edilmiş olmakla beraber, sertifika kullanıcısının iddia ettiği kişi olduğuna dair güvence sağlamak için net bir şekilde tanımlanmış bir sertifika üretim süreci vasıtasıyla ilave bir koruma seviyesi oluşturur.
GSSL sertifikalarının amacı, kullanıcılara gerçek ve yasal web sitelerini oltalama saldırısı yapan sitelerden net bir şekilde ayırma imkânı sağlamaktır ve çevrimiçi ticari işlemlere karşı güvenlerini arttırmaktır.
GSSL sertifikaları günümüzde yaygın olarak kullanılmakta ve belli başlı web tarayıcıları tarafından tanınmaktadır.

7.2. Standart SSL sertifika üretim ve dağıtım şartları

Standart SSL sertifikalarının kullanımı Madde 7.1. de belirtilen hususlarda da belirtildiği üzere düşük güvenlik seviyesine haiz olduğundan dolayı, bu program kapsamında kamu kurumlarına yönelik olarak Standart SSL Sertifikası üretimi ve satışı **yapılmamalıdır**. Belirtilen bu şart nedeniyle bu program, Standart SSL sertifikalarına yönelik herhangi bir tasarrufta bulunmaz. Özel sektör kuruluşlarına yönelik olarak ise Standart SSL Sertifikası üretimi ve satışının yapılması tavsiye edilmez.

7.3. Kod İmzalama Sertifikaları

Kod imzalama sertifikaları üreten SSHS lar ve ürettikleri sertifikalar da bu program kapsamında aynı idari ve teknik kriterlere tabidir.

7.4 Güvenli SSL Sertifika üretim ve dağıtım şartları

SSL Sertifika Hizmet Sağlayıcısı bir kuruluşu hangi sertifikaları yayımlayacağı konusunda yetkilendirmek için ilave adımlar gerçekleştirdiğinde, yayımlanmış sertifikalar ayırt edilir ve genişletilmiş onay sertifikaları yayımlanır. Bu sertifikalar web sayfası sahiplerinin kimliğine ilişkin daha fazla güvence sağlar.

“Güvenli SSL (GSSL) Sertifikaları mevcut SSL sertifika formatı üzerine yapılır, ancak sertifika sahibi olduğunu iddia edenlerden emin olmak için oluşturulmuş katı tanımlı yayımlama sürecinde tanımlanmış ilave bir koruma katmanı sağlar. Devam etmekte olan sürecin bütünlüğünü sağlamak için, yürürlükten kaldırma ölçümleri hatalı yayımlanmış veya yanlış kullanılmış sertifikaların hızlı ve etkili iptali için izin vermesi belirtilir. İleri Gelen Güvenilen Taraf Uygulama Yazılımı Sağlayıcıları Web sayfası sahibinin onaylanmış kimliğini görüntülemek için tarayıcıya izin veren GSSL i destekler.”

7.4.1 SSHS Güvenli SSL Sertifikası iş uygulamalarının duyurulması

SSHS, Güvenli SSL sertifikası uygulama esasları ve prosedürlerini ve TSE tarafından yayınlanan bu programa uyumluluk sağlamaya yönelik taahhüdünü kamuoyuna duyurur.

1. SSHS'nin SM'mı ve onun Kök SM'mı web sayfası üzerinden aşağıdaki bilgileri duyururlar:

    - Güvenli SSL Sertifika uygulama esasları, İlkeleri ve prosedürleri,
    - Güvenli SSL Sertifika yayınlayan SM ile aynı Nesne Adına sahip hiyerarşik yapıdaki SM ler ve
    - SSHS'nin TSE tarafından yayınlanan bu programa uyumluluk sağlamaya yönelik taahhüdü

2. SSHS Güvenli SSL Sertifikaların iptal edilmesi için izlenmesi gereken yolları duyurur.

3. SSHS, SM tarafından yayınlanan Güvenli SSL Sertifikalar ile ilgili şikâyet veya şüphe edilen özel anahtar çalınması, Güvenli SSL Sertifikası suiistimali veya diğer dolandırıcılık, suiistimal veya uygun olmayan kullanım tiplerinin müşterilerine, ilgili taraflara, uygulama yazılım üreticilerine ve diğer 3.cü taraflara bildirimine yönelik talimatlar sağlar.

4. SM ve Kök SM, RFC 2527 ya da RFC 3647 ye göre yapılandırılmış olan Sertifika İlkeleri ve/veya Sertifika Uygulama Esaslarına yedi gün yirmi dört saat açık erişim sağlanmasını makul güvence seviyesinde temin etmek için kontrollere sahip olmalıdır.

7.4.2. Güvenli SSL Sertifikaları Kriterleri

GSSL sertifikalarının temel amacı TLS/SSL protokolleri ile web iletişiminin ve çalıştırılabilir kodların güvenliğinin sağlanmasıdır. Bunu yaparken aşağıdakileri temin etmek önem arz etmektedir:

Bir web sitesinin sahibi olan veya kontrol eden yasal kuruluşun tespit edilmesi: Bir Internet tarayıcısının kullanıcısına, erişmekte olduğu web sitesinin GSSL sertifikasında yer alan Ad, İş yeri adresi, Kayıt bilgisi, Kayıt numarası vb. ile tanımlanmış belirli bir yasal kuruluş tarafından kontrol edildiğinin yeterli derecede güvencesinin sağlanması.

Bir web sitesi ile şifreli iletişimin sağlanması: Bir Internet tarayıcısı kullanıcısı ile bir web sitesi arasında bilgilerin şifreli iletiminin sağlanması amacıyla şifreleme anahtarlarının değiştirilmesi.

Yukarıda tanımlı uygulamaların gerçekleştirilebilmesi için en yaygın olarak kullanılan tarayıcılar ve SSHS'ler tarafından oluşturulmuş olan CA/Browser Forum adı altında bir organizasyon kurulmuş ve bu organizasyon tarafından Güvenli SSL sertifikalarına ait kriterler belirlenmiştir.

SSHS'lerin yayınladıkları sertifikaların Internet tarayıcıları tarafından GSSL olarak tanınabilmesi için SSHS lerin yayınladıkları GSSL sertifikaların CAB Forum tarafından yayınlanan kriterlere uyum sağlamaları ve onaylanmış olması gerekmektedir. Aksi takdirde SSHS lerin yayınlamış olduğu sertifikalar Internet tarayıcılar tarafından GSSL olarak kabul edilmemektedir.

Bu noktadan hareketle bu program kapsamında yayınlanan GSSL sertifikalarının da CAB Forum tarafından yayınlanan kriterlere uyum sağlamış ve onaylanmış olması uygun görülmüştür.

SSHS'lerin bu program kapsamında, CAB Forum şartlarına uyum sağlamalarının yanı sıra, bu programda belirtilen diğer şartları da karşılamaları gerekmektedir.

8. Kanunlara ve mevzuata uyum

SSHS'ları 04/05/2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele edilmesi Hakkında Kanun" a tabidirler.

9. Kaynakça

[1] TS ISO/IEC 27001, Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

[2] Open Web Application Security Project http://www.owasp.org

[3] How-digital-certificates-are-used-and-misused
http://blog.zeltser.com/post/56162725038/how-digital-certificates-are-used-and-misused

[4] Why Doesn't DigiCert Offer DV SSL? http://www.digicert.com/dv-ssl-certificate.htm

[5] CA/Browser Forum Guidelines for the issuance and management of Extended Validation Certificates

[6] ETSI 101 456 Policy Requirements for Certification Authorities issuing qualified certificates