FIPS 140 STANDARDI

ÖNER ZİYA BAŞ

Kriptoloji ve Güvenlik Protokolleri

Nisan 2021

İçindekiler

1. FIPS 140 STANDARDI

1.1. GİRİŞ

Çağlar boyunca bilgi güvenliği insanlar ve toplumlar arasında daima önemli bir yer almış, sadece yetkilendirilmiş kişilerin bilmesi gereken sırlar çeşitli yöntemlerle korunmaya çalışılmıştır. Teknoloji öncesi kullanılan her sistem kendi içinde sorgulanırken teknolojinin gelişmesi ve yaygınlaşması ile bilgi teknolojilerinde kullanılan bileşenlerin güvenilirliği de bu ürünlerin kullanılmasıyla birlikte tartışılmaya başlamıştır.

Günümüzde devletler, kurumlar ve insanlar kritik altyapı ve sistemlerde kullanılan bilgiyi korumak için kriptografiye güvenmektedir. Bu ürün ve sistemlerde, gizlilik, bütünlük, inkâr edememe ve kimlik doğrulama gibi kriptografik hizmetleri sağlamak için kriptografik modüller kullanılmaktadır. Devletler, kurumlar ve insanlar, test edilmiş ve onaylanmış ürünleri kullanmak ister ve bundan fayda sağlarlar. Yeterli test yapılmayan, zayıf tasarım ve algoritma içeren veya kriptografik modülün yanlış uygulanmasından doğan sonuçlar güvensiz ürünlerin ortaya çıkmasına yol açar.

Bilgi teknolojilerinde kullanılan bileşenlerin güvenilirliğini sağlamak, gereksinimlerini belirlemek, onaylanmasını ve doğrulanmasını sağlamak vb. gibi işlemleri yapmak ve bunu uluslararası bir düzeyde geçerli kılmak için bazı standartlar ortaya çıkmıştır. İşte bunlardan biri olan **FIPS (Federal Information Processing Standard) 140** standardı (Şifreleme Modülleri için Güvenlik Gereksinimleri), kriptografik modüllerin tasarlanmasında, uygulanmasında ve çalıştırılmasında kullanılmasının yanı sıra modüllerin test edilmesi ve doğrulanması için de yöntemler tanımlamaktadır.

Kriptografik modül, şifreleme, şifre çözme, dijital imzalar, kimlik doğrulama teknikleri ve rasgele sayı üretimi gibi kriptografik işlevleri uygulayan donanım ve veya yazılım olarak tanımlanır. Bu modüller yaptıkları işi eksiksiz ve aksatmadan yapmalıdır.

NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından yayınlanan **FIPS 140 Standart** serisi, ABD devlet daireleri ve kurumları tarafından kullanılmak üzere hem donanım hem de yazılım bileşenlerini içeren kriptografik modüller için gereksinimleri belirlemek ve standartları koordine etmek amacını taşımaktadır. Standart herkese açıktır ve isteyen uygulayabilir.

2. FIPS 140 STANDARTLAR SERİSİ

2.1. TARİHÇE

Serinin ilk yayını olan FIPS 140-1 11 Ocak 1994 tarihinde yayınlanmıştır. 25 Mayıs 2002'de sona eren bir geçiş döneminin ardından yerini FIPS 140-2'ye bırakmıştır. Kullanımda olan sürümler FIPS 140-2 ve FIPS 140-3'tür.

Standart kullanıcılardan ve satıcılardan oluşan bir hükümet ve endüstri çalışma grubu tarafından geliştirilmiştir. Çalışma grubu, geniş bir uygulama (örneğin, düşük değerli idari veriler, yüksek değerli fon transferleri vb.) ve ortam yelpazesi (örneğin, korumalı bir tesis, bir ofis veya tamamen korumasız bir konum) sağlamak amacıyla kriptografik modül gereksinimleri için dört güvenlik seviyesi belirlemiştir. Her güvenlik seviyesi, önceki seviyeye göre güvenlikte bir artış sunmaktadır. Bu dört artan güvenlik seviyesi, farklı veri hassasiyeti dereceleri ve farklı uygulama ortamları için uygun olan uygun maliyetli çözümlere izin vermektedir.

Yukarıda da belirtildiği gibi bilgi sistemlerinde kullanılan kriptografik modüller sağladığı hizmete göre (anahtar yönetimi, e-imza, şifreleme vb.) farklı güvenlik gereksinimlerine ihtiyaç duyabilir. Gereksinimler, yalnızca kriptografik modüllerin kendisini değil, aynı zamanda belgelerini ve kaynak kodda bulunan yorumların bazı alanlarını da kapsar. Bu alanlar arasında temel tasarım ve belgelendirme, modül arayüzleri, yetkili roller ve hizmetler, fiziksel güvenlik, yazılım güvenliği, işletim sistemi güvenliği, anahtar yönetimi, kriptografik algoritmalar, elektromanyetik girişim / elektromanyetik uyumluluk (EMI / EMC) ve kendi kendine testler yer alır. FIPS 140 Standardı, kendi gereksinimlerine uyan bir modülün güvenli olduğunu garanti etmez.

FIPS 140-1, NIST'in en başarılı standartlarından birisidir ve **Kriptografik Modül Doğrulama Programı**nın (**CMVP**) temelini oluşturur. FIPS 140-1, kriptografik modüller için "defacto" standart olarak yaygın bir şekilde tanınmış ve çok sayıda standart kuruluşu ve uluslararası test kuruluşu tarafından referans alınmış ve /veya bütünüyle kullanılmıştır.

İhtiyaçlar doğrultusunda standardın geliştirmesi gerektiğinden akıllara şu soru gelmiştir. "Başarılı ve kanıtlanmış bir standart nasıl geliştirilir?" İşte FIPS 140-2, sorulardan ve yorumlardan çıkarılan dersler ele alınarak ve teknolojideki değişiklikler de eklenerek yazılmıştır. 140-1'in içeriği minimum düzeyde yeniden yapılandırılmış, gereksiz bilgileri kaldırmış, açıklık ve tutarlılık sağlamak için kullanılan dil ve terminoloji standartlaştırılmış ve standardın formatı iyileştirilmiştir. Ayrıca şu anda özel testleri bulunmayan kriptografik modüllere yönelik yeni saldırı türlerini detaylandıran yeni bir bölüm eklenmiştir. Böylece standart daha da güçlendirilmiş, ancak odak veya vurgu değişmemiştir.

FIPS 140-3 bir kriptoprafik modülün tasarım aşamasından başlayarak uygulama ve son dağıtıma kadar uzanan güvenlik gereksinimlerini tanımladığı için daha geniş bir tehdit ve güvenlik açığı yelpazesini kapsar. FIPS 140-3, daha önce var olan iki uluslararası standart olan ISO / IEC 19790: 2012 "Şifreleme Modülleri için Güvenlik Gereksinimleri" ve ISO 24759: 2017 "Kriptografik Modüller için Test Gereksinimleri" ni temel alır.

Üreticiler şu anda bir şifreleme modülünü FIPS 140-2 veya FIPS 140-3'e göre doğrulayabilirler. İki sürüm eşdeğerdir ve FIPS 140-2'yi seçmenin herhangi bir sakıncası yoktur.

FIPS 140-1 yayından kaldırıldığı için güvenlik Seviyeleri FIPS 140-2 standardına göre incelenmiştir.

3. FIPS 140 GÜVENLİK SEVİYELERİ

3.1. SEVİYE 1

Bu seviye bir kriptografik modül için belirlenen en düşük düzeydeki temel güvenlik gereksinimlerini belirtir. Seviye 1, üretim sınıfındaki bileşenler için temel gereksinimlerin ötesinde hiçbir fiziksel güvenlik mekanizması gerektirmez ve bir kriptografik modülün değerlendirilmemiş bir işletim sistemi kullanılarak genel amaçlı bir bilgisayarda yürütülmesine izin verir.

Güvenlik Düzeyi 1 şifreleme modülüne bir örnek, kişisel bir bilgisayardaki (PC) bir şifreleme kartıdır.

Seviye 1'de yer alan bazı önemli noktalar.

- Kriptografik modül, onaylı çalışma modunda en az bir adet onaylı güvenlik işlevi uygulamalıdır. Onaylanmamış güvenlik işlevleri onaylı olmayan çalışma modlarına dahil edilebilir. Operatör, onaylı çalışma modunun ne zaman seçileceğini belirleyebilmelidir.
- Bir kriptografik modül, tüm bilgi akışını (şifreleme anahtarları ve bileşenlerinin, kimlik doğrulama verilerinin modüle giden ve modüle gelen tüm giriş ve çıkış noktaları) fiziksel bağlantı noktaları ve mantıksal arabirimlerle (örneğin, aynı port üzerinden giriş verileri girebilir ve çıkış verileri çıkabilir) sınırlandırmalıdır. Fiziksel bağlantı noktaları ve mantıksal arabirimler, kriptografik modüldeki diğer bağlantı noktaları ve arabirimlerle fiziksel ve mantıksal olarak paylaşılabilir.
- Kriptografik modül, operatörler için aşağıdaki yetkili rolleri desteklemelidir: Kullanıcı rolü, Kripto Görevlisinin Rolü, Bakım Rolü. Kriptografik modül tarafından desteklenen tüm yetkili roller dokümantasyonda yer almalıdır.
- Kriptografik modül, operatörlere şu hizmetleri sağlamalıdır: Şifreleme modülünün mevcut durumu gösterilmeli, kendi kendine testler yapabilmeli ve en az bir onaylı güvenlik işlevi gerçekleştirmeli. Hizmetler, kriptografik modül tarafından gerçekleştirilebilecek tüm işlemlere veya işlevlere atıfta bulunmalı, her hizmet girdisi bir hizmet çıktısı ile sonuçlanmalıdır.
- Modüle erişimi denetlemek için kimlik doğrulama mekanizmalarının kullanıldığı bir şifreleme modülü gerekmez. Kimlik doğrulama mekanizmaları şifreleme modülü tarafından desteklenmiyorsa, modül bir veya daha fazla rolün operatör tarafından örtük veya açıkça seçilmesini gerektirir.
- Şifreleme modülünün çalışması, durum geçiş diyagramı ve/veya durum geçiş tablosu tarafından temsil edilen sonlu bir durum modeli (veya eşdeğeri) kullanılarak belirtilmelidir.
- Bir kriptografik modülün işletim ortamı, modülün çalışması için gerekli olan yazılım ve / veya donanım bileşenlerinin yönetimini ifade eder. İşletim ortamı değiştirilemez (ROM) veya değiştirilebilir (RAM) olabilir. Güvenlik Düzeyi 1'de işletim sistemi tek bir operatör çalışma modu ile sınırlandırılmıştır. Kriptografik modül, şifreleme modülünün çalıştığı süre boyunca diğer işlemlerin düz metin özel ve gizli anahtarlara, ara anahtar oluşturma değerlerine vb. erişimini engellemelidir. Kriptografik modül tarafından oluşturulan işlemler modüle aittir ve yürütme sırasında kriptografik olmayan işlemler tarafından kesintiye uğramamalıdır. Tüm kriptografik yazılımlar, yürütülebilir kodu yetkisiz ifşa ve değişikliklere karşı koruyan bir biçimde kurulmalıdır. Onaylanmış bütünlük tekniğini kullanan bir kriptografik mekanizma (örneğin, onaylanmış mesaj kimlik doğrulama kodu veya

dijital imza algoritması), kriptografik modül içindeki tüm kriptografik yazılım ve ürün yazılımı bileşenlerine uygulanmalıdır.

- Anahtar yönetimi, rastgele sayı ve anahtar oluşturma, anahtar dağıtımı, anahtar giriş / çıkış işlemleri, anahtar depolama ve anahtar sıfırlamayı da içeren bir yaşam döngüsü içinde yapılır. Gizli anahtarlar, özel anahtarlar ve kritik güvenlik parametreleri, yetkisiz ifşa, değişiklik ve değiştirmeye karşı şifreleme modülü içinde açık anahtarlar ise kriptografik modül içinde korunmalıdır. Gerektiğinde kriptografik modül başka bir kriptografik modülün anahtar yönetim mekanizmalarını da kullanabilir. Algoritmada kullanılan sayılar gerekli testlerden geçmiş rastgele sayı üretme fonksiyonları ile sağlanmalıdır. Bu fonksiyonlarda kullanılan geri besleme değeri vb. değerlere de yetkisiz erişim engellenmelidir ve gizli kalmalıdır. Güvenlik Seviyesi 1 ve 2 için, otomatikleştirilmiş yöntemler kullanılarak oluşturulan gizli ve özel anahtarlar, kriptografik modüle şifrelenmiş biçimde girmeli ve çıkmalıdır. Manuel yöntemler kullanılarak oluşturulan gizli ve özel anahtarlar, şifreleme modülüne düz metin biçiminde girilebilir veya buradan çıkarılabilir.

3.2. SEVİYE 2

Seviye 1'e ilave üç ana gereksinim eklenmiştir.

- Kriptografik modüle yapılacak bir fiziksel müdahaleyi tespit edebilmek için fiziksel kilit (koruma kaplaması, conta vb.) veya kurcalama karşıtı mühürler kullanılmalıdır.
- Şifreleme modülü modüle erişimi denetlemek için rol tabanlı kimlik doğrulaması kullanacaktır.
- Kriptografik modülün onaylanmış veya değerlendirilmiş güvenilir bir işletim sisteminden yararlanan genel amaçlı bir bilgisayarda yürütülmesine izin verir. İşletim sistemleri Ortak Kriterler (CC) değerlendirme güvence seviyesi EAL2 veya daha yüksek bir seviyede değerlendirilmelidir.

3.3. SEVİYE 3

Seviye 2' ye ilave dört ana gereksinim eklenmiştir.

- Saldırganın kriptografik modül içindeki kritik güvenlik parametrelerine erişimini önlemek için fiziksel güvenlik sağlanmalıdır. Kurulacak mekanizmanın amacı kriptografik modüle fiziksel olarak yetkisiz erişim, kurcalama veya kullanma girişimlerini tespit etme ve bunlara tepki verme olasılığını yükseltmektir. Herhangi bir kurcalama tespit edilirse, cihaz kritik güvenlik parametrelerini silebilmelidir.
- Şifreleme modülü modüle erişimi denetlemek için rol tabanlı kimlik doğrulamadan daha ayrıntılı bir kimlik doğrulama yöntemi olan kimlik tabanlı kimlik doğrulama mekanizması kullanmalıdır. Bu, belirli bir kullanıcının rolünü doğrulamak yerine belirli bir kullanıcının kimliğini doğrulayarak elde edilir.
- Düz metin şifreleme anahtarı bileşenlerinin, kimlik doğrulama verilerinin ve kritik güvenlik parametrelerin girişi ve çıkışı için kullanılan bağlantı noktaları fiziksel veya mantıksal olarak (örneğin, güvenilir bir yol veya doğrudan bağlanan kablo aracılığıyla) ayrılmalıdır.
- İşletim sistemi gereksinimleri Seviye 2'den daha katıdır ve bir CC değerlendirme güvence düzeyi EAL3 veya daha üstünü içerir. Güvenlik Düzeyi 3 işletim sistemi gereksinimleri hakkında daha fazla bilgi FIPS 140-2 yayınında Bölüm 1.3'te bulunabilir.

3.4. SEVİYE 4

Bu seviye diğer güvenlik düzeylerinden daha yüksek düzeyde güvenlik sağlar ve fiziksel olarak korumasız ortamlarda çalışan kriptografik modüller için idealdir. Fiziksel olarak korunmasız ortamlara örnek olarak uydular ve insansız hava araçları verilebilir. Güvenlik Düzeyi 4'ün amacı, şifreleme modülünü tüm yetkisiz fiziksel erişim girişimlerine karşı korumasını sağlamaktır. Mekanizmalar, bir saldırı tespitinde çok yüksek bir olasılık sağlamalı ve bir saldırı tespit edilmesi durumunda tüm düz metin kritik güvenlik parametrelerini derhal sıfırlayacak şekilde tasarlanmalıdır.

Elektronik cihazlar ve devreler, belirli bir çevre koşulları aralığında çalışmak üzere tasarlanmıştır. Belirtilen normal çalışma voltaj ve sıcaklık aralıkları dışındaki kasıtlı veya kazara gezintiler, şifreleme modülünün güvenliğini tehlikeye atabilecek elektronik cihazların veya devrelerin hatalı çalışmasına veya arızalanmasına neden olabilir. Bir kriptografik modülün güvenliğinin aşırı çevresel koşullar tarafından tehlikeye atılamayacağına dair makul güvence, modülün çevresel arıza koruma (EFP) özelliklerini kullanması veya çevresel hata testine (EFT) tabi tutulmasıyla sağlanabilir. Güvenlik Düzeyi 4'te, bir kriptografik modül ya çevresel arıza koruma (EFP) özelliklerini kullanacak ya da çevresel hata testine (EFT) tabi tutulacaktır.

Saldırganlar modülün güvenliğini tehlikeye atmak için şifreleme modülünü normal voltaj ve sıcaklığının dışına itme yöntemini (aşırı ısıtma veya soğutma) yaygın olarak kullanmaktadır.

Kriptografik modül normal çalışma aralığı dışındaki dalgalanmaları tespit ederse, çevre koruma önlemleri kritik güvenlik parametrelerini sıfırlayabilir. Örneğin saldırgan sıvı nitrojen kullanarak kriptografik modüldeki kilidi dondurmak ve kırmak için müdahalede bulunduğunda çevre koruma önlemleri kilidin belirlenen bir eşiğin altındaki sıcaklığa maruz kaldığını tespit eder ve modülü sıfırlar. Bu noktadan sonra saldırgan modüle erişse bile işine yaramaz.

İşletim sistemi gereksinimi daha üst bir seviyeye taşınmıştır. Bir şifreleme modülünün FIPS 140-2 Seviye 4 uyumlu olması için, üzerinde çalıştığı işletim sisteminin EAL4 veya daha yüksek bir CC değerlendirmesi alması gerekir.

4. FIPS 140 SERTİFİKASI

4.1. FIPS 140 SERTİFİKASI NEDEN ALINIR?

Bir ürünün FIPS 140 sertifikasına sahip olması için birçok neden vardır, ancak gerçekten zorlayıcı olan tek şey yasal düzenlemelerdir. Birçok hükümet sözleşmesi, örneğin kablosuz cihazlar veya şifreli sabit sürücüler için belirli FIPS seviyelerinin sertifikalandırılmasını gerektirir. Bununla birlikte özellikle finans, sağlık, eğitim ve altyapı (ulusal güvenlik) şirketleri FIPS 140 uyumu talep etmektedirler.

Sertifika almak için daha az zorlayıcı sebep ise, FIPS 140'ın bir kalite işareti olarak görülebilmesidir. Pazarlama aracı olarak kullanılabilir. FIPS 140'a sahipseniz ve rakipleriniz yoksa, rekabet avantajınız olabilir.

4.2. FIPS 140 SERTİFİKALI OLMAK

NIST 17 Temmuz 1995 tarihinde, şifreleme modüllerini FIPS 140 ve diğer FIPS şifreleme tabanlı standartlara göre doğrulayan CMVP (Şifreleme Modülü Doğrulama Programı) programını kurarak, doğrulanmış ürünlerin kullanımını teşvik etmek ve federal kurumlara kriptografik modüllerin tedarikinde kullanılacak bir güvenlik seviyesi sağlamak istemiştir.

Belirli bir şifreleme modülünün FIPS 140 ile uyumlu olduğunun doğrulanması için, bir kuruluş bu modülü Şifreleme Modülü Doğrulama Programına (CMVP) sunmalıdır.

Modüllerinin CMVP tarafından değerlendirilmesi için bir kuruluş, modülü akredite bir Kriptografik Modül Test Laboratuvarına sunmalıdır. Akredite laboratuvarlar, Ulusal Gönüllü Laboratuvar Akreditasyon Programı (NVLAP) tarafından onaylanmış üçüncü taraf laboratuvarlardır.

Dileyen herkes, **CMVP Onaylı Modüller Listesi**nden sorgulama yapabilir ve ürünlerin iddia edilen güvenlik düzeyini karşılayıp karşılamadığını kontrol edebilir. CMVP, altta yatan standartların, test metodolojisinin, raporlama yapısının ve ilgili dokümantasyonun sürekli olarak incelenmesi sebebi ile dinamik bir yapıya sahiptir.

4.3. FIPS 140 SERTİFİKASTONUN SÜRDÜRÜLMESİ

FIPS 140 sertifikası uzun ve zaman alıcı bir süreç olabilir. Ek olarak, ne kadar küçük olursa olsun, yazılımda yapılan her değişiklik için modül yeniden değerlendirilmelidir. FIPS uyumlu bir modülde bir sorun keşfedilirse, çözüm yeniden değerlendirilip onaylanana kadar FIPS sertifikasını kaybeder. Bu süre zarfında kuruluş, modüllerini standardı talep eden satıcılara ve acentelere sağlayamayacaktır.

4.4. FIPS 140 SERTİFİKASININ ELEŞTRİLEN YÖNLERİ

Doğrulama sürecinin uzun olması can sıkıcıdır. Aylarca süren doğrulama süreci ve her değişiklik için ürünlerini yeniden doğrulaması gerektiği gerçeği nedeniyle, birçok şirket bir hata tespit edilse bile yazılımı güncelleme veya yükseltme konusunda isteksizdir. Bu, kritik güncellemelerde geride kalmaya neden olabilir ve hatta kuruluşları kodlarındaki küçük hataları gizlemeye teşvik edebilir.

Örneğin, bir kuruluş, sertifikalı bir modülde bir güvenlik açığı keşfetti ve yamayı aynı gün dağıtıma hazır hale getirdi, ancak yamayı gereken sürede doğrulayamadı. Sonuç, kuruluşun yazılımlarındaki güvenlik açığını duyurması ve CMVP'nin modülün FIPS 140 doğrulamasını neredeyse anında iptal etmesi ve yeni doğrulama tamamlanana kadar onları ve müşterilerini belirsizlik içinde bırakması.

Standart kapsamında sadece ABD-NIST tarafından onaylanmış algoritmalar değerlendirilir.

5. SONUÇ

Bu çalışmada kriptografik modüllerin güvenlik gereksinimlerini tanımlayan FIPS PUB 140 standardı incelenmiştir.

Birçok kullanıcının güvenlik ihtiyacı FIPS sertifikasına sahip olmayan cihazlar tarafından karşılanmaktadır. Örneğin bir USB bellek herhangi bir FIPS sertifikasına sahip olmayabilir, ancak yine de kurumsal düzeyde donanım şifrelemesine, merkezi yönetime ve fiziksel kurcalamaya karşı sağlamlığa sahip olabilir.

Tüketici tarafından bakıldığında yasal zorunluluklar ve şartlar dışarıda bırakıldığında çok az kullanıcı 3. seviyeyi karşılayan güvenlik özelliklerine ihtiyaç duyar ve çoğunluk 2. seviyeye ihtiyaç duymaz. Seviye arttıkça maliyet de artacağı için ürünün satış fiyatı da artar.

Seviyelerle ilgili bir örnek verecek olursak seviye 2 ile sertifikalandırılmış bir sabit disk düşünelim. Birisi sürücüyü fiziksel olarak açmaya çalışırsa, kurcalama kanıtları gösterecektir. Seviye üçte ise birisi sürücüye fiziksel olarak girmeye çalıştığında verilerin kilidini açmak için kullanılan şifreleme “anahtarları” yok edilecektir.

Kriptografi uygulayan ürünlerin satışı için FIPS 140 sertifikasına sahip değilseniz veya en azından bir sertifika alma taahhüdünüz yoksa, ürününüzü bu önemli pazarda satamama ihtimaliniz yüksektir.

6. TANIMLAR VE KAYNAKÇA

6.1. TANIMLAR

Kritik Güvenlik Parametresi (CSP) - NIST Sözlüğü'ne göre CSP'ler, ifşa edilmesi veya değiştirilmesi bir kriptografik modülün güvenliğini tehlikeye atabilecek güvenlikle ilgili bilgileri içerir.

Ortak Kriterler (CC) - Bilgi Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriter olarak da bilinir. Güvenlik ürünlerinin bağımsız lisanslı laboratuvarlar tarafından yeterince test edilmesini sağlayan uluslararası bir anlaşma olan Ortak Kriterler Tanıma Düzenlemesi' nin (CCRA) teknik temeli olarak hizmet eder.

6.2. KAYNAKÇA

- Kripto (TS ISO/IEC 19790-24759) https://tse.org.tr/IcerikDetay?ID=2059
- Federal Information Processing Standard (FIPS) 140-1 https://csrc.nist.gov/csrc/media/publications/fips/140/1/archive/1994-01-11/documents/fips1401.pdf
- Federal Information Processing Standard (FIPS) 140-2 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- Federal Information Processing Standard (FIPS) 140-3 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
- A COMPARISON OF THE SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES IN FIPS 140-1 AND FIPS 140-2 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151243
- Cryptographic Module Validation Program https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules
- Kriptografik Modüllerin Güvenlik Gereksinimleri https://iscturkey.org/assets/files/2016/03/2008-posters-02.pdf
- What is FIPS 140-2 Compliance? https://www.xmedius.com/en/blog/what-is-fips-140-2-compliance/
- Understanding The New FIPS 140-3 https://www.cryptomathic.com/news-events/blog/understanding-the-new-fips-standard-fips-140-3
- FIPS 140-2 Standart ve Kendinden Şifreli Disk Teknolojisi https://www.seagate.com/tr/tr/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/