ORTAK KRİTERLER KORUMA PROFİLİ

GÜVENLİ EM (IC) PLATFORMU

Taslak Versiyon 1.0

TÜRK STANDARDLARI ENSTİTÜSÜ

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

1. GİRİŞ

1 . 1 KP Referansı

1.1.1BAŞLIK

Güvenli IC Platformu

1.1.2SÜRÜM

Taslak

1.1.3YAZAR

Türk Standartları Enstitüsü

1.1.4 YAYIN TARİHİ

.------

1.2DH GENEL BAKIŞ

1.2.1 DH TİPİ

DH, akıllı kart uygulamaları için yürütme ortamını oluşturan Güvenli IC'dir.

Paket, pil ve anten gibi harici bileşenler ve fiziki kart KP'nin kapsamı dışındadır. Paketleme ve bileşik ürün üretimi de değerlendirme içeriğinden çıkarılmıştır. Tek gerekliliğin, DH'nin bileşik ürün üretimine güvenli teslim edilmesi ve üretiminden güvenli teslim alınması olduğu varsayılmıştır. DH'nin teslimat güvenliği de bileşik ürün değerlendirmesi kapsamındadır.

1.2.2DH KULLANIMI VE TEMEL GÜVENLİK ÖZELLİKLERİ

DH, aşağıda belirtilmiş olan güvenlik duyarlı uygulamalar için bir platform olarak kullanılmaktadır:

- Tanılama ve Kimlik Doğrulama
- Elektronik Ödeme ve Cüzdan
- Elektronik İmza
- Güvenli Veri Depolama

DH, uygulama verisini ve tümleşik işletim sistemini saldırganlara karşı korur ve tümleşik sisteminin doğru çalıştırılmasını sağlar. DH ayrıca, tümleşik işletim sistemi için "Rastgele Sayı Üretimi" güvenlik hizmetini de sağlar.

DH'nin karşı koyacağı tehditler ve tümleşik işletim sisteminin sahip olması gereken özellikler, bu KP'nin Güvenlik Sorunu Tanımı kısmında belirtilmiştir. Ancak devam etmeden ve detaylara girmeden önce, DH'nin hedefi, uygulamalar ve tüketiciler için, platformu hedef alan saldırılara karşı dirençli bir güvenli platform sağlamaktır.

Yürürlükteki KP, ROM tabanlı ve Flaş tabanlı olmak üzere DH'nin iki farklı konfigürasyonunu ele almaktadır. Aradaki fark yaşam döngüsündeki değişikliklerden ortaya çıkmakta ve Flaş tabanlı teknolojinin sunduğu esneklik ek güvenlik kaygılarına neden olmaktadır.

Yürürlükteki Koruma Profili, güvenlik sorununu, ortam için güvenlik hedeflerini ve güvenlik gereksinimlerini tanımlamaktadır. Güvenlik sorunu, DH ile etkileşimde olan harici öğeleri, varlıkları, ortamla bağlantılı güvenlik hizmetlerini, tehditleri, varsayımları ve DH'nin uyumlu olması gereken kurumsal güvenlik politikalarını tanımlar. Ortam, üretim tesisi, son-kullanıcı ortamı ve kart yayınlayıcısı ortamından oluşur. DH açısından, kart yayınlayıcısı ve son kullanıcı ortamı arasındaki fark sadece ve sadece DH flaş tabanlıysa ve flaş yükleyici, üreticiden kart yayınlayıcısına teslim edilmeden önce devreden çıkarılmadıysa ortaya çıkar. Ortam için güvenlik hedefleri, DH'nin güvenli olması için ortamdan beklenen unsurları ortaya koyar. Son kullanıcı ortamından bir beklenti yoktur ve akıllı kart uygulamalarının yapısına bağlı olarak tamamının saldırgan bir ortam olduğu varsayılmaktadır. Ancak üretim ve kart yayınlama tesislerinden beklentiler mevcuttur. Nihayetinde KP'de, hem fonksiyonel güvenlik gereksinimleri hem de güvenlik garanti gereksinimleri verilmiştir. Güvenlik hedeflerinin güvenlik sorununu nasıl çözdüğünün rasyoneli ve güvenlik gereksinimlerinin DH güvenlik hedeflerini nasıl yerine getirdiğinin rasyoneli de belirtilmiştir.

1.2.3 DH DONANIMI/DONANIM YAZILIMI/YAZILIMI

Yok

1.3 DH TANIMI

1.3.1 DH KONFİGÜRASYONLARI

Bu KP'de mevcut olan tümleşik OS depolama teknolojisi seçimine bağlı olarak iki farklı DH konfigürasyonu bulunmaktadır:

- ROM Tabanlı
- Flaş Tabanlı

ROM Depolama: Bu konfigürasyon, Tümleşik OS'nin DH'nin üretiminden önce teslim edilmesini gerektirmektedir. Tümleşik OS, DH'nin ROM Hafızasında depolanmıştır ve yeniden yazmak mümkün değildir.

Flaş Depolama: Flaş Teknolojisi sayesinde tümleşik OS DH üretildikten sonra yüklenir. Bu konfigürasyon içindeki DH'nin için Flaş Yükleyici Yazılımı bulunmaktadır ve tümleşik OS'nin Flaş Hafızaya yüklenmesi işlevini sağlar. Tümleşik OS'yi yüklemek için birçok seçenek vardır; üretici tümleşik OS'yi yükleyebilir ve Kart Yayınlayıcısına teslim etmeden önce flaş yükleyiciyi devreden çıkarabilir veya DH Es olmadan teslim edilir ve flaş yükleyici devrededir.

Farklı konfigürasyonları yaşam döngülerinden başlayarak, iki konfigürasyon için farklar bu KP içinde mevcuttur. Bu nedenle, bu KP'yle uyumlu olduğunu iddia eden herhangi bir DH, desteklediği tümleşik OS depolama teknolojisinin ***Rom-tabanlı*** veya ***Flaş Tabanlı*** olup olmadığını KP uyumluluk beyanında belirtmelidir.

DH konfigürasyonu, tümleşik işletim sisteminin nasıl depolandığı ya da yüklendiğine bağlı olarak farklılık gösterir. Tümleşik işletim sistemi üretim esnasında, DH üretiminden önce hazırlanmış olan Hard ROM maskeleri kullanılarak gömülebilir veya DH Flaş Teknoloji tabanlıysa bir flaş yükleyici programı vasıtasıyla üretimden sonra yüklenebilir. Flaş veya ROM teknolojisinin kullanımı,

DH'nin yaşam döngüsünü değiştirir ve Flaş Teknolojisi, esnekliğine bağlı olarak Flaş tabanlı DH'ler için ek güvenlik kaygılarına neden olur. Bu KP ile uyumlu olduğunu iddia eden bir DH için, bu DH'nin desteklediği teknoloji güvenlik hedefinde belirtilmelidir.

Bu KP'de belirtilmiş olan konfigürasyonların yanı sıra, ilave tehditler, kurumsal güvenlik politikaları, DH güvenlik hedefleri ve güvenlik gereksinimleri ilave edilebilir. Varsayımlara ve ortamsal güvenlik hedeflerine yapılacak herhangi bir ilave, KP'nin diğer öğeleriyle tutarlı olmalıdır.

Konfigürasyonlar için Not:

ROM tabanlı teknoloji daha basittir ve ROM tabanlı ve Flaş tabanlı DH arasındaki tek fark, Flaş tabanlı DH'nin ek güvenlik unsurlarına sahip olmasıdır. Bu nedenler, ilk olarak ROM tabanlı teknolojinin SPD'leri, GH'leri ve GG'leri verilmiş ve daha sonra var ise Flaş tabanlı DH için ek unsurlar belirtilmiştir.

1.3.2 DH İÇERİĞİ

DH

- Güvenlik IC Donanımı
- Güvenlik IC Özgül Yazılımı
- IC Eşsiz Tanımlama Verisi + Konfigürasyon Verisi (opsiyonel)
- Güvenlik Kılavuz Dokümantasyonu

Donanım: Donanım; CPU'dan, geçici ve geçici-olmayan belleklerden, I/O bileşenlerinden ve güvenlik bileşenlerinden oluşmaktadır.

Güvenlik IC Özgül Yazılımı: Tümleşik OS dışındaki herhangi bir yazılım, Güvenlik IC Özgül Yazılımıdır. Güvenlik IC Özgül Yazılımı; IC Özgül Test Yazılımı, IC Özgül Destek Yazılımı ve tümleşik OS Flaş Bellekte depolandıysa ilave Flaş Yükleyici Yazılımından oluşmaktadır.

IC Eşsiz Tanımlama Verisi: Eşsiz tanımlama, kart yayınlayıcısının gereksinimidir.

Konfigürasyon Verisi (opsiyonel)**:** IC üreticileri tüketicilerine, farklı boyutlardaki belleklere ve farklı işlevselliklere sahip geniş bir ürün yelpazesi sunar. Ürün çeşitliliği sağlamak için genellikle, farklı konfigürasyonlara sahip aynı fiziksel ürünü kullanırlar. İşlevsellikleri devre dışı bırakmak için mekanizmalarla ve bellek boyutunu ve/veya işlevsellikleri kısıtlayan ya da bloke eden bazı konfigürasyon verileriyle farklı konfigürasyonlar uygulanır. Bir bayi aynı fiziksel ürünün faklı konfigürasyonlarını sunmayabilir, bu durumda konfigürasyon verisi mevcut değildir ve bu nedenle opsiyoneldir.

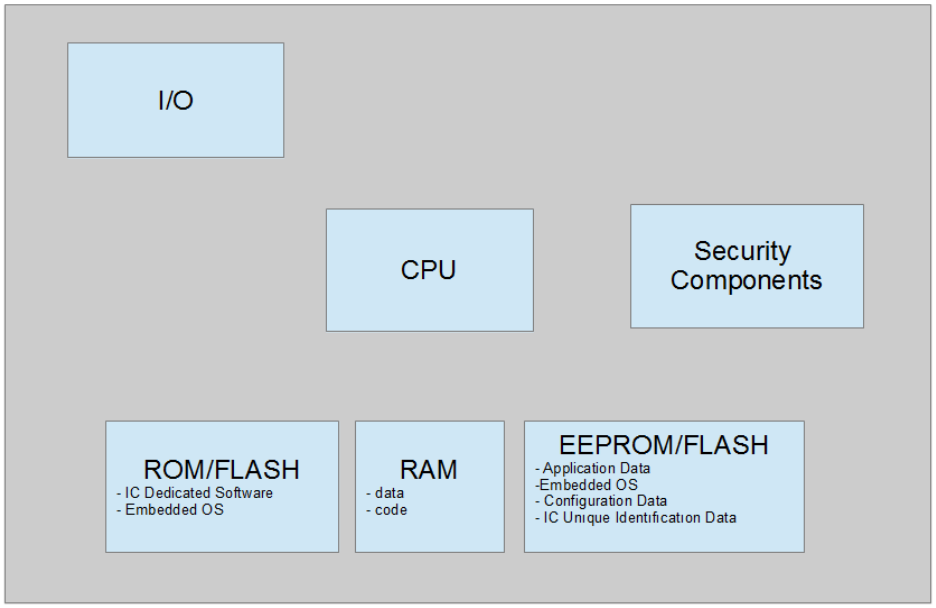
Güvenlik Kılavuz Dokümantasyonu: IC'nin güvenli kullanımı hakkında bilgileri içerir. Güvenlik Kılavuz Dokümantasyonu, sadece ve sadece DH'nin belgelendirilmiş olduğu düşünülen bu güvenlik kılavuzuna uygun şekilde kullanılması durumunda değerlendirilir. Güvenlik kılavuzuna herhangi bir uyumsuzluk, güvenlik sertifikasını bozacak DH'nin değerlendirilen konfigürasyon durumunda olduğu varsayılabilecektir.

1.3.3DH FİZİKSEL GÖRÜNÜMÜ

Fiziksel Donanım şunlardan oluşur:

- CPU
- Değişken ve Değişken-olmayan Bellekler

- Güvenlik Bileşenleri
- İletişim Arayüzleri



Şekil 1: Güvenli IC Diyagramı

Değişken-olmayan Belleklerde Depolanan Veriler

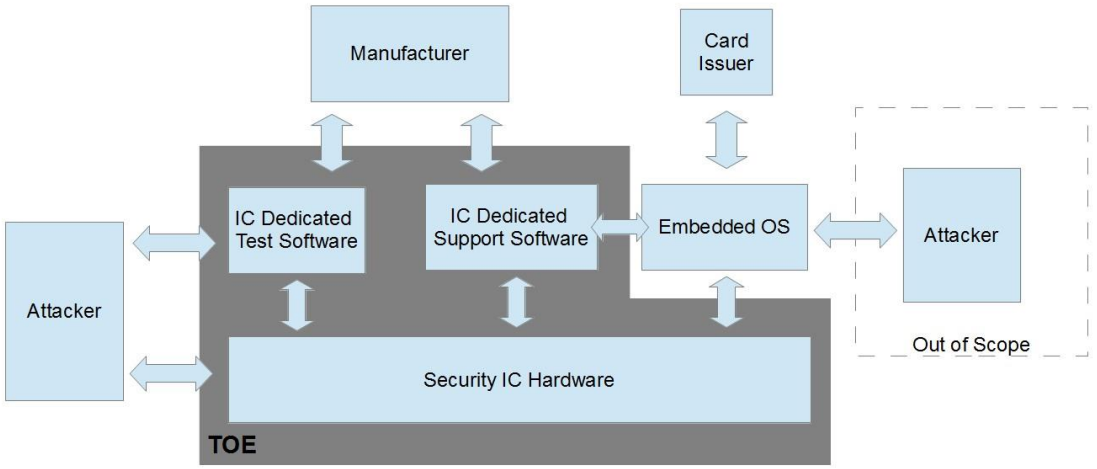
- IC Özgül Yazılım
- Tümleşik OS
- Uygulama Verisi
- Konfigürasyon Verisi
- IC Eşsiz Tanılama Verisi

Ayrı Olarak Teslim Edilen Kalem(ler):

- Kılavuz Belgeleri

1.3.4 LOJİK GÖRÜNÜM

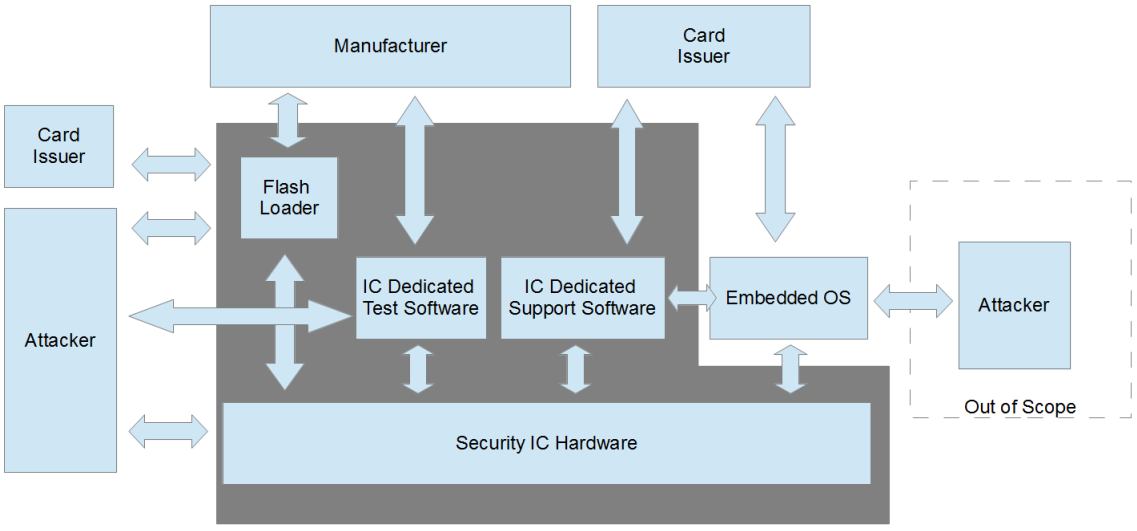
DH'nin lojik görünümü aşağıdaki şekil 2'de verilmiştir. IC Özgül Test Yazılımı, IC Özgül Destek Yazılımı ve IC Donanımı hep birlikte DH'ni oluşturur ve sınırlarını belirler. İşletim aşamasında DH, tümleşik OS ve saldırgan ile etkileşime girer ve tümleşik OS'yi saldırgandan korur. Teslimat öncesi, DH üreticisi IC Özgül Test Yazılımı ve IC Özgül Destek Yazılımı ile etkileşim içindedir.



Şekil 2: ROM tabanlı konfigürasyon için DH'nin Lojik Görünümü

1.3.4.1 FLAŞ TABANLI DH'NİN LOJİK GÖRÜNÜMÜ

Flaş tabanlı DH için, Flaş Yükleyici yazılımı DH içinde ilaveten yer alır. Kart yayınlayıcı üreticisi, DH'ye tümleşik işletim sistemini yüklemek için Flaş Yükleyiciyi kullanır ve teslimat öncesi ileride kullanılmak üzere flaş yükleyicinin kilidini açar. Saldırgan ayrıca, flaş yükleyicinin sunduğu işlevselliği istismar etmek ve kendi tümleşik işletim sistemini yüklemek için flaş yükleyiciyle etkileşime girebilir. Aşağıda, flaş tabanlı DH için lojik diyagram verilmiştir.



Şekil 3: Flaş tabanlı DH için Lojik Model

1.3.5 DH YAŞAM DÖNGÜSÜ MODELİ

1.3.5.1 YAŞAM DÖNGÜSÜNÜN AŞAMALARI

DH'nin yaşam-döngüsü içerisinde aşağıdaki aşamalar bulunmaktadır*:

- Tasarım ve Geliştirme Aşaması
- Üretim Aşaması
- Kart Yayınlayıcı Aşaması

* Akıllı kartın fiziksel özelliklerinin kapsamı dışında uygulama yaptıkları için paketleme ve bileşik ürün üretimi dışarıda bırakılmıştır.

Akıllı kart uygulamalarından ve tümleşik işletim sistemlerinden kaynaklanan gereksinimler, geçmiş yıllarda çok iyi tanımlandığından ve olgunlaştığından, gereksinimler aşaması hariç tutulmuştur.

Tasarım ve Geliştirme Aşaması:

Bu aşamada, DH'nin tasarımı ve IC Özgül Yazılım'ın (flaş tabanlı olması durumunda ayrıca flaş yükleyicinin) geliştirilmesi yerine getirilir. Tasarım verisi ve yazılım üretim aşamasına teslim edilir. Ayrıca, kılavuz belgeler de tümleşik işletim sistemi geliştiricisine teslim edilir.

Üretim Aşaması:

Üretim aşaması esnasında, ROM tabanlı durumlarda tümleşik işletim sistemi Tümleşik OS Geliştiricisinden alınır ve DH;

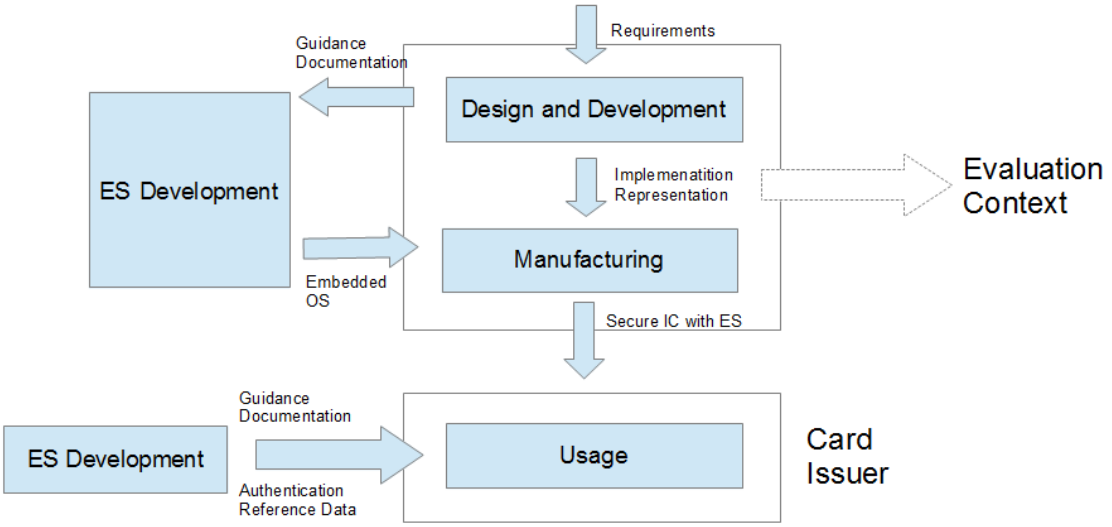
- üretilir (ROM tabanlı durumlarda tümleşik işletim sistemi de içine konulur);
- test edilir (hatalı olanlar belirlenir ve ayıklanır)
- test işlevselliği devreden çıkarılır
- tümleşik işletim sistemi yüklenir (flaş tabanlı olanlar için ve tümleşik işletim sistemi üretici tarafından yüklendiyse; tümleşik işletim kart yayınlayıcı tarafından yüklendiyse bu adım hariç tutulur)
- flaş yükleyici devreden çıkarılır (flaş tabanlı olanlar için ve tümleşik işletim sistemi üretici tarafından yüklendiyse; tümleşik işletim kart yayınlayıcı tarafından yüklendiyse bu adım hariç tutulur)
- IC Eşsiz tanılama yazılır
- DH Kart Yayınlayıcıya teslim edilir.

Kart Yayınlayıcı Aşaması:

- DH üreticiden teslim alınır (ROM tabanlı durumlarda ve flaş tabanlı durumlar için eğer tümleşik işletim sistemi üretici tarafından DH'ye yüklendiyse, DH, tümleşik işletim sistemiyle beraber gelir)
- Kart Yayınlayıcı tümleşik işletim sistemini DH'ye yükler (Kart Yayınlayıcının tümleşik işletim sistemini yüklediği durumlarda) ve flaş yükleyiciyi devreden çıkarır
- Artık DH'nin tek kullanıcısı tümleşik işletim sistemidir ve saldırgan kart yayınlayıcının güvenlik politikasını deneyebilir.

1.3.5.2 ÜRETİCİ ES'Yİ YÜKLER YAŞAM-DÖNGÜSÜ MODELİ

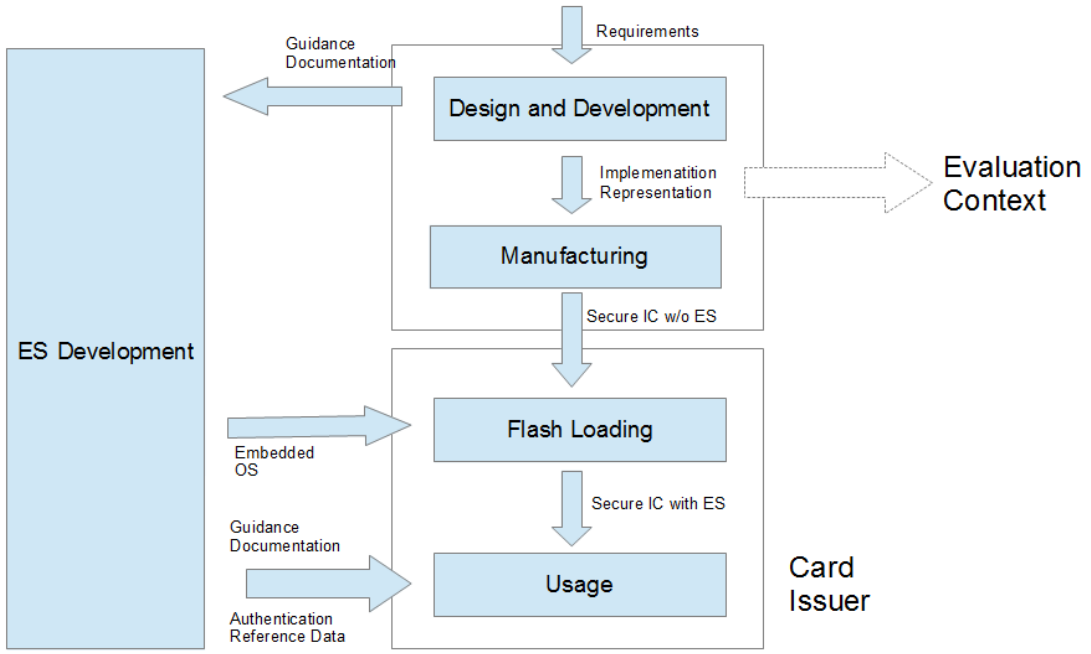
Bu yaşam-döngüsü, ES Geliştirici ES'yi DH'ye koyduğu zaman gerçekleşir. Yaşam-döngüsü açısından, Flaş veya ROM teknolojisinin kullanılmasının bir farkı yoktur çünkü her iki durumda da DH, Kart Yayınlayıcıya ES yüklenmiş ve ES yeniden yükleme devreden çıkarılmış şekilde teslim edilir.



Şekil 4: Üretici ES'yi yükler Yaşam-döngüsü

1.3.5.3 KART YAYINLAYICI ES'Yİ YÜKLER YAŞAM-DÖNGÜSÜ MODELİ

Bu durumda, DH üreticiden ES yüklenmemiş şekilde ve flaş yükleyici işler durumda teslim alınır. Tümleşik işletim sistemini yüklemek ve tümleşik işletim sisteminin yüklenmesinden sonra flaş yükleyiciyi devreden çıkarmak kart yayınlayıcının sorumluluğundadır.



Şekil 5: : Kart Yayınlayıcı ES'yi yükler Yaşam-döngüsü

2. UYUMLULUK İDDİLARI

2.1 OK UYUMLULUK İDDİASI

Bu Koruma Profili, aşağıdaki hususlara uyumlu olduğunu iddia etmektedir:

- Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 1: Giriş ve Genel Model; CCMB-2012-09-001, Sürüm 3.1, Revizyon 4, Eylül 2012
- Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 2: Fonksiyonel Güvenlik Gereksinimleri; CCMB-2012-09-002, Sürüm 3.1, Revizyon 4, Eylül 2012
- Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 3: Güvenlik Garanti Gereksinimleri; CCMB-2012-09-003, Sürüm 3.1, Revizyon 1, Eylül 2012

Ayrıca

- Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Metodoloji (CEM), Değerlendirme Metodolojisi; CCMB-2012-09-004, Sürüm 3.1, Revizyon 4, Eylül 2012

De dikkate alınmalıdır.

2.2 KP İDDİASI

Bu KP herhangi bir başka KP'ne uyumluluk iddiasında bulunmaz.

2.3 PAKET İDDİASI

Bu KP, OK Kısım 3'te tanımlanan ALC_DVS.2 ve AVA_VAN.5 ile ilave edilmiş EAL5 garanti paketiyle uyumludur.

2.4 UYUMLULUK BEYANI

Bu Koruma Profili, GH veya bu KP'ye uyumlu olduğunu iddia eden KP için **kesin** uyumluluk gerektirmektedir.

3.GÜVENLİK SORUNU TANIMI

3.1GİRİŞ

3.1.1VARLIKLAR VE GÜVENLİK HİZMETLERİ

Korunması gereken varlıklar ve verilecek ve korunacak güvenlik hizmetleri şunlardır: **Uygulama Verisi** (varlık) Ve **Rastgele Sayı Üretimi** (güvenlik hizmeti).

Uygulama Verisi: Uygulama verisi, ES'ye ait olan ve ES tarafından yönetilen tüm verilerdir.

Rastgele Sayı Üretimi: DH, kullanıcılarına (burada sadece ES), rastgele sayı tedarik eder. Rastgele sayılar, ES'nin hizmet verdiği güvenlik uygulamaları için şarttır.

Varlıkların ve güvenlik hizmetlerinin yanı sıra, **IC Eşsiz Tanılama Verisi** ve **ES** olan TSF Verilerinin de DH tarafından korunması gereklidir. Tüm üretilen ve Kart Yayınlayıcıya teslim edilen ürünlerin Eşsiz Tanılaması, kurumsal güvenlik politikasından kaynaklanan bir gerekliliktir: O.Eşsiz_Tanılama. Değişken-olmayan bellekte depolanan ES de, ifşa edilmeye veya manipülasyona karşı korunmalıdır. ES'nin manipülasyonu, DH'nin esas güvenlik konularından birinin ihlali olacak şekilde ES'nin hatalı işlev görmesiyle sonuçlanır. ES'nin ifşa edilmesi saldırganlara mühendislik ES'sini geriye çevirme ve zaaflarını keşfetme şansı verir.

İlave Kalemler:

Herhangi bir güvenlik hizmeti ve o güvenlik hizmetine ait olan TSF verisi, GH yazarı tarafından eklenebilir.

3.1.2KİŞİLER VE HARİCİ ÖĞELER

Üretici: Üretici DH'nin tasarımını, geliştirilmesini ve üretimini gerçekleştirir. Üretici ayrıca, şu yönetimsel eylemleri de yerine getirir: test fonksiyonlarının devreden çıkarılması, IC eşsiz Tanılama Verisinin yazılması, ES'nin yüklenmesi ve Flaş Yükleyicin devreden çıkarılması. ES'nin yüklenmesi ve Flaş Yükleyicinin devreden çıkarılması, DH flaş tabanlıysa ve ES yükleme üretici tarafından gerçekleştirildiyse yalnızda üretici tarafından yerine getirilir. ROM tabanlı durumlar için bu eylemler mevcut değildir ve kart yayınlayıcının ES'yi yüklediği durumlarda bu eylemler Kart Yayınlayıcı tarafından gerçekleştirilir.

ES: ES DH'nin tek kullanıcısıdır. DH ES'ye, güvenli bir uygulama ortamı ve verisinin güvenli depolanmasını sağlayarak hizmet sunar. DH ayrıca, kendisinin eşsiz tanılamasını ve rastgele sayıları da sağlar.

Kart Yayınlayıcı: Kart yayınlayıcı, DH'nin meşru sahibidir. Normalde DH'yi, tümleşik OS vasıtasıyla kullanır. Kart yayınlayıcı, DH'nin ES'ye güvenli uygulama ortamı ve güvenli depolama sağlaması hususlarında DH'ye güvenir. DH flaş tabanlıysa ve ES Kart Yayınlayıcı tarafından yüklendiyse, o zaman şu yönetimsel eylemleri gerçekleştirir: ES'yi yüklemek ve Flaş Yükleyiciyi devreden çıkarmak.

Saldırgan: Saldırgan, kart yayınlayıcının güvenlik politikalarını zayıflatmaya çalışan varlıktır. Saldırganın *yüksek saldırı potansiyeline* sahip olduğu varsayılmaktadır.

3.2TEHDİTLER

SONDA VE MANİPÜLASYON TEHDİTLERİ:

T.Veri_Depolamaya_Sonda: Bir saldırgan, uygulama verisine yasadışı erişim elde etmek için DH'nin belleklerine fiziksel olarak saldırabilir.

T.Veri_Transferine_Sonda: Bir saldırgan, uygulama verisine yasadışı erişim elde etmek için DH'nin dâhili bileşenlerine sonda yapabilir.

T.Veri-Depolama_Manipülasyonu: Bir saldırgan, uygulama verilerinde değişiklik yapabilmek için DH'nin belleklerine fiziksel olarak saldırabilir.

T.Veri_Transferi_Manipülasyonu: Bir saldırgan, DH'nin dâhili kısımları arasında transfer edilen uygulama verilerinde değişiklik yapabilmek için DH'nin dâhili bileşenlerine fiziksel olarak saldırabilir.

T.Uygulama_Manipülasyonu: Bir saldırgan, ES'nin uygulanmasını değiştirmek için CPU işletimine fiziksel olarak saldırabilir.

T.RS_Manipülasyonu: Bir saldırgan, DH'nin yetersiz kalitede rastgele sayı üretmesi için rastgele sayı dağıntısına fiziksel olarak saldırabilir.

SIZINTI VE EMİSYON (SALIM) TEHDİTLERİ

T.Bilgi_Sızdırma_Yüzey: Bir saldırgan, uygulama verisini ifşa etmek için DH'nin fiziksel yüzeyinden sızan salımları izleyip oynayabilir.

T.Bilgi_Sızdırma_Kişiler: Bir saldırgan, uygulama verisiyle oynamak ve erişim sağlamak için enerji tüketimi, işletim zamanlaması ve diğer gözlenebilir unsurları izleyebilir.

ORTAMSAL STRES TEHDİTLERİ

T.Ortamsal_Stres_Uygulaması: Saldırgan, DH'nin arıza yapması için standart işletim koşulları dışında sıcaklık, frekans, voltaj vs uygulayabilir.

FONKSİYONELLİK SUİİSTİMALİ TEHDİTLERİ

T.Test_Fonksiyonlarının_İstismarı: Saldırgan, uygulama verisine yasadışı erişim elde etmek için test fonksiyonlarını kullanmaya çalışabilir.

FLAŞ YÜKLEME KONFİGÜRASYONU İÇİN TEHDİT

T.Flaş_Yükleme_İstismarı: Saldırgan, Flaş Yükleyicinin işlevselliğini kullanarak ES'ye yapay bir ES yüklemeye çalışabilir. ***(Flaş tabanlı DH'ler için geçerlidir.)***

3.4 KURUMSAL GÜVENLİK POLİTİKALARI

P.IC_Eşsiz_Tanılama_Verisi: DH ES tarafından eşsiz olarak tanılanmalıdır.

P.Rastgele_Sayı_Üretimi: DH ES'ye rastgele sayılar tedarik etmelidir.

FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN KURUMSAL GÜVENLİK POLİTİKASI

P.Tümleşik_OS_Yüklemesi: DH Kart Yayınlayıcıya veya Üreticiye, ES yükleme imkânı sağlamalıdır.

3.5 VARSAYIMLAR

A.Kılavuz_Doküman_Uyumluluğu: ES'nin, DH'nin güvenlik kılavuzu ile uyumlu olduğu varsayılmıştır. DH'nin güvenliği ES'ye bağlıdır ve sadece ve sadece ES doğru kullanırsa etkili olacak güvenlik mekanizmaları olabilir.

4.1 DH İÇİN GÜVENLİK HEDEFLERİ

OT.Veri_Erişim_Kontrolü: DH, DH üzerinde depolanan ve işlenen verileri, fiziksel sonda vasıtasıyla yetkisiz erişimlere karşı korumalıdır. Belleklere erişim sadece ES'ye verilmelidir. Yetkisiz erişim, bir saldırgan tarafından gerçekleştirilebilecek fiziksel sondayı kapsar.

OT.Veri_Bütünlüğü: DH, DH üzerinde depolanan verinin manipülasyonunu tespit etmelidir.

OT.Dâhili_DH_Aktarım_Gizliliği_Koruması: DH, DH'nin dâhili kısımları arasında aktarılan verilerin gizliliğini, sondaya karşı korumalıdır.

OT. Dâhili_DH_Aktarım_Bütünlüğü_Koruması: DH, DH'nin dâhili kısımları arasında aktarılan verilerin bütünlüğünü korumalıdır.

OT.CPU_İşletim_Koruması: DH'nin, tümleşik OS uygulamasına karşı herhangi bir manipülasyona karşı koruma için işlevselliğe sahip olması gereklidir.

OT.Rastgele_Sayı_Üretimi_Koruması: DH'nin, rastgele sayı üretimi işlevini korumak için işlevselliğe sahip olması gereklidir.

OT.Ortamsal_Stres_Koruması: DH'nin kendisini ortamsal strese karşı koruması için mekanizma(lar)a sahip olması gereklidir.

OT.Yan_Kanallı_Koruma: DH, T.Bilgi_Sızıntısı_Kişiler tehdidine karşı korumaya sahip olmalıdır.

OT.Test_Fonksiyonları_Devreden_Çıkarma_Mekanizması: DH'nin, üreticinin test işlevselliğini geri dönülemez şekilde devreden çıkarmasını sağlayan mekanizmalara sahip olması gereklidir.

OT.Rastgele_Sayı_Üretimi: DH'nin, tümleşik işletim sistemine rastgele numaralar sağlaması için mekanizmalara sahip olması gereklidir.

OT.Eşsiz_Tanılama_Depolama: DH'nin, Eşsiz Tanılama Verilerini depolaması için bir işlevselliğe sahip olması gereklidir. Bu veri sadece üretici tarafından yazılabilir olmalıdır.

FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN EK HEDEFLER

OT.Flaş_Yükleyici_İşlevselliği: DH, tümleşik işletim sistemi yükleme işlevselliğine sahip olmalıdır.

OT.Flaş_Yükleyici_Yetkilendirme: DH flaş yükleyicinin kullanılması için sadece yetkilendirilmiş varlıklara izin vermelidir.

OT.Flaş_Yükleyici_Devreden_Çıkarma_Mekanizması: DH'nin, üreticinin ve/veya kart yayınlayıcının flaş yükleyici işlevselliğini geri dönülemez şekilde devreden çıkarabilmesini sağlayan mekanizmalara sahip olması gereklidir.

4.2 ORTAM İÇİN GÜVENLİK HEDEFLERİ

OE.Test_Fonksiyonları_Devreden_Çıkarma: Üretici, teslimat öncesi her DH için test fonksiyonunun devreden çıkarıldığından emin olmalıdır.

OE.Eşsiz_Tanılama: Üretici, DH'nin eşsiz ID depolama mekanizmasını düzgün şekilde kullanmalıdır. Üretici, DH'lere yazılan ID'lerin eşsiz olduğunu temin etmelidir.

OE.Tümleşik_OS: Tümleşik işletim sistemi güvenlik kılavuzuyla uyumlu olmalıdır.

FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN EK HEDEFLER

OE.Flaş_Yükleyici_Devreden_Çıkarma: DH'nin yaşam-döngüsüne bağlı olarak, ya üretici ya da kart yayınlayıcı, teslim edilen her bir DH için flaş yükleyici işlevinin devreden çıkarıldığını temin etmelidir.

4.3 GÜVENLİK HEDEFLERİ RASYONELİ

4.3.1 GÜVENLİK HEDEFLERİ RASYONEL TABLOSU

Aşağıdaki tablo, güvenlik hedefleri kapsamı için genel bir bakış sağlamaktadır.

No	SPD	GH
1.	T.Veri_Depolamaya_Sonda	OT.Veri_Erişim_Kontrolü
2.	T.Veri_Aktarımına_Sonda	OT.Dâhili_DH_Aktarım_Gizliliği_Koruması
3.	T.Veri_Depolama_Manipülasyonu	OT.Veri_Erişim_Kontrolü, OT.Veri_Bütünlüğü
4.	T.Veri_Aktarımı_Manipülasyonu	OT.Dâhili_DH_Aktarım_Gizliliği_Koruması, OT.Dâhili_DH_Aktarım_Bütünlüğü_Koruması
5.	T.Uygulama_Manipülasyonu	OT.CPU_İşletim_Koruması
6.	T.RS_Manipülasyonu	OT.Rastgele_Sayı_Üretimi_Koruması
7.	T.Bilgi_Sızdırma_Yüzey	OT. Dâhili_DH_Aktarım_Gizliliği_Koruması
8.	T.Bilgi_Sızdırma_Kişiler	OT.Yan_Kanallı_Koruma
9.	T.Ortamsal_Stres_Uygulaması	OT.Ortamsal_Stres_Koruması
10.	T.Test_Fonksiyonlarının_İstismarı	OT.Test_Fonksiyonları_Devreden_Çıkarma_Mekanizması OE.Test_Fonksiyonları_Devreden_Çıkarma
11.	P.IC_Eşsiz_Tanılama_Verisi	OT.Eşsiz_ID_Depolama, OE.Eşsiz_Tanılama
12.	P.Rastgele_Sayı_Üretimi	OT. Rastgele_Sayı_Üretimi
13.	A.Kılavuz_Belgeleri_Uyumluluğu	OE.Tümleşik_OS

Tablo 1:Güvenlik Hedefleri Rasyoneli

FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN EK RASYONELLER

14.	P.Tümleşik_OS_Yükleme	OT.Flaş_Yükleyici_İşlevselliği
15.	T.Flaş_Yükleyicinin_İstismarı	OT.Flaş_Yükleyici_Yetkilendirme, OT.Flaş_Yükleyici_Devreden_Çıkarma_Mekanizması OE.Flaş_Yükleyici_Devreden_Çıkarma

Tablo 2:Flaş Yükleyici için Ek Rasyoneller

4.3.2 GÜVENLİK SORUNU GEREKÇESİ

Bu kısımda, güvenlik hedeflerine göre güvenlik sorunu gerekçesi sunulmuştur.

- **T.Veri_Depolamaya_Sonda**

OT.Veri_Erişim_Kontrolü, DH üzerinde depolanan ve işlenen verileri fiziksel sondaya karşı korur ve böylece OT.Veri_Erişim_Kontrolü hedefi T.Veri_Depolamaya_Sonda tehdidine karşı koyar.

- **T.Veri_Aktarımına_Sonda**

OT.Dâhili_DH_Aktarım_Gizliliği_Koruması, DH'nin dâhili parçaları arasında aktarılan verilerin gizliliğini korur ve böylece T.Veri_Aktarımına_Sonda tehdidini kapsar.

- **T.Veri_Depolama_Manipülasyonu**

OT.Veri_Bütünlüğü, DH üzerinde depolanan ve işlenen verilerin bütünlüğü, fiziksel manipülasyona karşı korur. Ve OT:Veri_Erişim_Kontrolü, verilerin okunmasına karşı koruma sağlar, saldırganın verinin fiziksel konumunu ve içeriğini öğrenmesini engeller. Böylece, OT.Veri_Erişim_Kontrolü sayesinde, OT.Veri_Bütünlüğü mevcut olmasa bile; bir saldırgan verileri manipüle eder ve yaptığı değişiklikleri öngöremez. OT.Veri_Bütünlüğü ve OT.Veri_Erişim_Kontrolü, bu tehdidi kapsar.

- **T.Veri_Aktarımı_Manipülasyonu**

OT.Dâhili_DH_Aktarım_Bütünlüğü_Koruması, DH'nin dâhili parçaları arasında aktarılan verilerin bütünlüğünü, fiziksel manipülasyona karşı korur. OT.Dâhili_DH_Aktarım_Gizliliği_Koruması saldırganın aktarımdaki veriyi riske atmasını engeller ve böylece makul değişiklikler mümkün olmaz. Böylece, OT.Veri_Erişim_Kontrolü sayesinde, OT.Veri_Bütünlüğü mevcut olmasa bile; bir saldırgan verileri manipüle eder ve yaptığı değişiklikleri öngöremez. OT.Veri_Bütünlüğü ve OT.Veri_Erişim_Kontrolü, bu tehdidi kapsar.

- **T.Uygulamanın_Manipülasyonu**

OT.CPU_İşletim_Koruması, CPU işletimlerini manipülasyondan korur. Bu şekilde, OT.CPU_İşletim_Koruması hedefi, T.Uygulama_Manipülasyonu tehdidini kapsar.

- **T.RS_Manipülasyonu**

OT.Rastgele_Sayı_Üretimi, Rastgele Sayı Üretimi işlevini, manipülasyondan korur. Bu şekilde, OT.Rastgele_Sayı_Üretimi_Koruması hedefi, T.RS_Manipülasyonu tehdidini kapsar.

- **T.Bilgi_Sızdırma_Yüzey**

OT.Dâhili_DH_Aktarım_Gizliliği_Koruması, aktarılan verinin gizliliğini korur ve bu sayede emisyonların yorumlanması imkânsız hale gelir. OT.Dâhili_DH_Aktarım_Gizliliği_Koruması bu tehdidi kapsar.

- **T. Bilgi_Sızdırma_Kişiler**

OT.Yan_Kanallı_Koruma, T. Bilgi_Sızdırma_Kişiler tehdidini kapsar.

- **T.Ortamsal_Stres_Uygulaması**

OT.Ortamsal_Stres_Koruması, T.Ortamsal_Stres_Uygulaması tehdidini kapsar.

- **T.Test_Fonksiyonlarının_İstismarı**

OT.Test_Fonksiyonları_Devreden_Çıkarma_Mekanizması, OE.Test_Fonksiyonları_Devreden_Çıkarma

- **T.Flaş_Yükleyicinin_İstismarı**

OT.Flaş_Yükleyici_Yetkilendirme, Flaş Yükleyicinin yetkisiz kişiler tarafından kullanılmasını engeller ve bu şekilde, teslimat esnasında veya kart yayınlayıcının tesislerinde saldırgan DH'ye erişim sağlasa bile, orijinal olmayan bir tümleşik işletim sistemi yüklemek için flaş yükleyiciyi kullanamayacaktır. OT.Flaş_Yükleyici_Devreden_Çıkarma_Mekanizması, üreticinin ya da kart yayınlayıcının, flaş yükleyici fonksiyonunu geri dönülemez şekilde devreden çıkarabilmesini sağlar. OE.Flaş_Yükleyici_Devreden_Çıkarma, üreticinin ya da kart yayınlayıcının (yaşam-döngüsü modeline bağlı olarak) flaş yükleyiciyi tesislerinde teslimattan önce devreden çıkarmaları gerektiğini deklare eder. Bu şekilde, OT.Flaş_Yükleyici_Yetkilendirme, OT.Flaş_Yükleyici_Devreden_Çıkarma_Mekanizması ve OT.Flaş_Yükleyici_Devreden_Çıkarma hedefleri bu tehdidi beraber kapsar.

- **P.IC_Eşsiz_Tanılama_Verisi**

OT.Eşsiz_ID_Verisi_Depolama, DH'nin ID depolama yetisini sağlar ve OE.Eşsiz_Tanılama, üreticinin DH için eşsiz bir tanılama verisi yaratmasını ve bunu kart yayınlayıcıya teslim etmeden önce DH'ye yazmasını gerektirir. Bu şekilde, OT.Eşsiz_ID_Depolama ve OE.Eşsiz_Tanılama, P.IC_Eşsiz_Tanılama_Verisi politikasını kapsar.

- **P.Rastgele_Sayı_Üretimi**

OT.Rastgele_Sayı_Üretimi, P. Rastgele_Sayı_Üretimi politikasını kapsar.

- **P.Tümleşik_OS_Yükleme**

OT.Flaş_Yükleyici_İşlevselliği, P.Tümleşik_OS_Yükleme politikasını kapsar.

- **A.Kılavuz_Dokümanları_Uyumluluğu**

A.Kılavuz_Dokümanları_Uyumluluğu, tümleşik işletim sisteminin, güvenlik kılavuz dokümanlarıyla uyumlu olduğunu varsayar; OE.Tümleşik_OS bu varsayımı yerine getirir.

5. GENİŞLETİLMİŞ BİLEŞENLER

Aşağıdaki bileşenler eklenmiştir:

- FCS_RND.1
- FPT_SCP.1

5.1 FCS SINIFI ŞİFRELEME DESTEĞİ

SOY FCS_RND RASTGELE SAYILARIN ÜRETİMİ

Soy davranışı:

Bu soy, şifreleme amacıyla kullanılmak istenen rastgele sayıların üretilmesi için kalite gereksinimlerini tanımlar.

Bileşen seviyeleme:

FCS_RND Generation of random numbers	1

FCS_RND.1 Rastgele sayıların üretimi, rastgele sayıların tanımlı bir kalite ölçevini karşılamasını gerektirir.

Yönetim: FCS_RND.1:

Öngörülen bir yönetim faaliyeti yoktur.

Denetim: FCS_RND.1

Denetlenebilir tarafından tanımlanmış bir eylem yoktur.

FCS_RND.1 Rastgele sayıları için kalite ölçevi

Hiyerarşi: Diğer bileşenlerle hiyerarşi yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FCS_RND.1.1 TSF, [atama: tanımlanmış bir kalite ölçevini] karşılayan rastgele sayıları üretmek için bir mekanizma sağlar.

5.2 TSF'NİN FPT SINIFI KORUNMASI

SOY FPT YAN KANALLI KORUMA

DH, saldırının DH'nin harici fiziksel fenomenlerine bağlı olduğu yerlerde DH ve diğer gizli verilere karşı yapılacak saldırıları engelleyecektir. Bu tip saldırıların örnekleri, DH'nin basit güç analizinin (SPA) değerlendirilmesi, farklılaştırılmış güç analizi (DPA), zamanlama saldırıları vs'dir. Bu soy, OK Kısım 2'nin başka bir bileşeninin doğrudan ele almadığı açık sızıntıların sınırlandırılması için fonksiyonel gereksinimleri açıklar.

“Yan Kanallı Koruma (FPT_SCP)” soyu, aşağıdaki şekilde belirlenmiştir.

Soy davranışı:

Bu soy, zaman ve güç analizi vasıtasıyla bilgi sızıntılarını azaltmak için gereksinimleri tanımlar.

Bileşen seviyeleme:

FPT_SCP: Yan Kanallı Koruma	1

FPT_SCP.1 Yan kanallı koruma, TSF verisine veya kullanıcı verisine erişimi sağlayan arayüz sızıntısının yayılmamasını gerektirir.

Yönetim: FPT_SCP.1

Öngörülen yönetim faaliyeti yoktur.

Denetim: FPT_SCP.1

Denetlenebilir tarafından tanımlanmış bir eylem yoktur.

FPT_SCP.1 Yan Kanallı Koruma

Hiyerarşi: Diğer bileşenlerle hiyerarşi yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_SCP.1 TSF, [atama: kullanıcıların tipinin], [atama: TSF verisi tipleri listesine] ve [atama: kullanıcı verisi tipleri listesine] erişim elde etmek için aşağıdaki [atama: bağlantı tipi] arayüzünü kullanamayacaklarını temin edecektir.

6. GÜVENLİK GEREKSİNİMLERİ

6.1 FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ

6.1.1 VERİ ERİŞİM KONTROLÜ VE AKTARIM KORUMASI

Sonda tehdidi, saldırgan fiziksel belleklere erişmeye çalışırken ve/veya DH'nin dâhili kısımları arasındaki veri trafiğini izlemeye çalışırken modellenebilir. "Veri Erişim Kontrolü" ve "Dâhili DH Aktarım Gizliliği Kontrolü" güvenlik hedefleri, DH'nin bu tip bir tehdide karşı koruma sağlaması gerektiğini belirler. Bu hedeflere, kısaca "TSF, belleklerde depolanan ve DH'nin dâhili kısımları arasında aktarılan tüm verilere erişim iznini sadece Tümleşik OS'ye (tek meşru kullanıcı) verir" şeklinde beyanat yapan ***Dâhili Veri Erişimi Politikasının*** yürürlüğe konmasıyla ulaşılabilir.

Dâhili Veri Erişimi Politikası, üç FGG ile yürürlüğe konulur: FDP_ACC.2, FDP_ACF.1 ve FDP_ITT.1. Hem FDP_ACF.1 hem de FDP_ITT.1 saldırganının tümleşik işletim sistemine erişimini, sistemi şifreleyerek engeller. Bu şekilde, şifreleme işletimlerine (şifre üretimi, şifreleme ve şifre çözme, şifre imhası) bağlıdırlar. FCS_CKM.1, FCS_CKM.4 ve FCS_COP.1 ayrıca, Sonda FGG'lerine karşı Korumaya da eklenir.

FDP_ACC.2 Tüm erişim kontrolü

Hiyerarşi: FDP_ACC.1 Alt küme erişim kontrolü

Bağımlılıklar: FDP_ACF.1 FDP_ACF.1 tarafından yerine getirilen güvenlik özniteliği tabanlı erişim kontrolü

FDP_ACC.2.1 TSF, *Dâhili Veri Erişim Politikasını*[1] *Saldırgan, Tümleşik OS* üzerinde ve *Uygulama Verisi*[2] *Dâhili Veri Erişim Politikasını*[1] *Saldırgan, Tümleşik OS* ve *Uygulama Verisi*[2] ve SFP tarafından kapsanan kişiler ve nesneler arasındaki tüm diğer işletimler için yürürlüğe koyacaktır.

FDP_ACC.2.2 TSF, TSF tarafından kontrol edilen tüm kişiler ve TSF tarafından kontrol edilen tüm nesneler arasındaki tüm işletimlerin bir erişim kontrolü FGG ile kapsanacağını temin edecektir.

FDP_ACF.1 Güvenlik özniteliği tabanlı erişim kontrolü

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FDP_ACC.1 FDP_ACC.2 tarafından yerine getirilen alt küme erişim kontrolü

FMT_MSA.3 Yerine getirilmeyen ancak gerekçelendirilen statik öznitelik ilklendirme

FDP_ACF.1.1 TSF, nesneler üzerinde *Dâhili Veri Erişimi Politikasını*[3] aşağıdakilere dayalı olarak yürürlüğe koyacaktır:

Saldırgan, Tümleşik OS ve Uygulama Verisi, kullanıcı tipi][4].

[1] [atama: erişim kontrolü SFP]
[2] [atama: kişilerin ve nesnelerin listesi]
[3] [atama: erişim kontrolü SFP]
[4] [atama: belirtilen SFP altında kontrol edilen kişilerin ve nesnelerin listesi ve her biri için ilgili SFP Güvenlik öznitelikleri veya adlandırılan SFP-bağlantılı güvenlik öznitelikleri grupları]

FDP_ACF.1.2 TSF, kontrol edilen kişiler ve kontrol edilen nesneler arasında bir işletime izin verilip verilmediğini belirlemek için aşağıdaki kuralları yürürlüğe koyacaktır:

- *Kişi Tümleşik OS ise erişime izin verilir*
- *Kişi Saldırgan ise erişime izin verilmez*

FDP_ACF.1.3 TSF, kişilerin nesnelere erişimine aşağıdaki ek kurallara bağlı olarak açık şekilde yetki Verecektir: *yok*[5].

FDP_ACF.1.4 TSF, kişilerin nesnelere erişimini aşağıdaki ek kurallara bağlı olarak açık şekilde engelleyecektir: *yok*[5].

FDP_ITT.1 Temel dahili aktarım koruması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FDP_ACC.1 Alt küme erişim kontrolü, veya FDP_ACC.1 tarafından yerine getirilen FDP_IFC.1 Alt küme bilgi akışı kontrolü

FDP_ITT.1.1 TSF, DH'nin fiziksel olarak ayrılmış kısımları arasında aktarımı yapılırken kullanıcı verisinin *ifşa edilmesini ve değiştirilmesini*[8] engellemek için *Dahili Veri Erişimi Politikasını* [7] yürürlüğe koyacaktır.

FDP_ITT.1 ayrıca, IC'nin fiziksel yüzeyi üzerindeki sızıntılar vasıtasıyla herhangi bir gizli veri sızıntısını engeller.

6.1.1.1 VERİ ERİŞİM KONTROLÜNE ŞİFRELEME DESTEĞİ VE AKTARIM KORUMASI

FCS_CKM.1/SP Kriptografik şifre üretimi – Depolama Koruması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FCS_CKM.2 Kriptografik şifre dağıtımı, veya

FCS_COP.1 FCS_COP.1/SP tarafından yerine getirilen Kriptografik işletim]

FCS_CKM.4 FCS_CKM.4 tarafından yerine getirilen Kriptografik şifre imhası

FCS_CKM.1.1 TSF, belirli bir kriptografik şifre üretimi algoritmasına [atama: kriptografik şifre üretimi algoritması][9] ve şunu karşılayan belirlenmiş kriptografik şifre boyutlarına [atama: kriptografik

[5] [atama: kişilerin nesnelere erişimine açık şekilde yetki veren güvenlik özniteliklerine dayalı olan kurallar]
[6] [atama: kişilerin nesnelere erişimini açık şekilde engelleyen güvenlik özniteliklerine dayalı olan kurallar]
[7] [atama: erişim kontrolü SFP(leri) ve/veya bilgi akışı kontrolü SFP(leri)]
[8] [seçim: ifşa, değiştirme, kullanım kaybı]
[9] [atama: kriptografik şifre üretimi algoritması]

şifre boyutları][10] göre kriptografik şifre üretimi yapacaktır: [atama: standartlar listesi][11]

FCS_CKM.1/TP Kriptografik şifre üretimi – Aktarım Koruması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FCS_CKM.2 Kriptografik şifre dağıtımı, veya

FCS_COP.1 FCS_COP.1/TP tarafından yerine getirilen Kriptografik işletim]

FCS_CKM.4 FCS_CKM.4 tarafından yerine getirilen Kriptografik şifre imhası

FCS_CKM.1.1 TSF, belirli bir kriptografik şifre üretimi algoritmasına [atama: kriptografik şifre üretimi algoritması][12] ve şunu karşılayan belirlenmiş kriptografik şifre boyutlarına [atama: kriptografik şifre boyutları][13] göre kriptografik şifre üretimi yapacaktır: [atama: standartlar listesi][14].

FCS_CKM.4 Kriptografik şifre imhası

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FDP_ITC.1 Kullanıcı verisinin güvenlik öznitelikleri olmadan alınması, veya

FDP_ITC.2 Kullanıcı verisinin güvenlik öznitelikleriyle alınması, veya

FCS_CKM.1 FCS_CKM.1 tarafından yerine getirilen Kriptografik şifre üretimi]

FCS_CKM.4.1 TSF, aşağıdakini karşılayan belirlenmiş bir kriptografik şifre imha metoduna [atama: kriptografik şifre imha metodu] [15] göre kriptografik şifreleri imha edecektir: [atama: standartlar listesi] [16].

FCS_COP.1/SP Kriptografik işletim – Depolama Koruması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FDP_ITC.1 Kullanıcı verisinin güvenlik öznitelikleri olmadan alınması, veya

FDP_ITC.2 Kullanıcı verisinin güvenlik öznitelikleriyle alınması, veya

FCS_CKM.1 FCS_CKM.1/SP tarafından yerine getirilen Kriptografik şifre üretimi]

FCS_CKM.4 FCS_CKM.4 tarafından yerine getirilen Kriptografik şifre imhası

[10] [atama: kriptografik şifre boyutları]
[11] [atama: standartlar listesi]
[12] [atama: kriptografik şifre üretimi algoritması]
[13] [atama: kriptografik şifre boyutları]
[14] [atama: kriptografik şifre boyutları]
[15] [atama: kriptografik şifre imha metodu]
[16] [atama: standartlar listesi]

FCS_COP.1.1 TSF *şifreleme ve şifre çözme işlemini*[17], aşağıdakini karşılayan belirlenmiş bir kriptografik algoritmaya [atama: kriptografik algoritma][18] ve kriptografik şifre boyutlarına [atama: kriptografik şifre boyutları][19] göre yapacaktır: [atama: standartlar listesi][20].

FCS_COP.1/TP Kriptografik işletim – Aktarım Koruması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FDP_ITC.1 Kullanıcı verisinin güvenlik öznitelikleri olmadan alınması, veya

FDP_ITC.2 Kullanıcı verisinin güvenlik öznitelikleriyle alınması, veya

FCS_CKM.1 FCS_CKM.1/SP tarafından yerine getirilen Kriptografik şifre üretimi]

FCS_CKM.4 FCS_CKM.4 tarafından yerine getirilen Kriptografik şifre imhası

FCS_COP.1.1 TSF *şifreleme ve şifre çözme işlemini*[21], aşağıdakini karşılayan belirlenmiş bir kriptografik algoritmaya [atama: kriptografik algoritma][22] ve kriptografik şifre boyutlarına [atama: kriptografik şifre boyutları][19] göre yapacaktır: [atama: standartlar listesi][23].

FPT_SCP.1 Yan Kanallı Koruma

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_SCP.1 TSF, *saldırganların*[25], *Veri Depolama Koruma şifrelerine, Veri Aktarım Koruması şifrelerine*[27] ve *Depolanmış Veri ve Aktarılmış Verilere*[28] erişim elde etmek için aşağıdaki arayüz *fiziksel kişileri*[26] kullanamayacağını temin edecektir.

6.1.2 MANİPÜLASYONA KARŞI KORUMA

FDP_SDI.2 Depolanmış veri bütünlüğü takibi ve eylem

Hiyerarşi: FDP_SDI.1 Depolanmış veri bütünlüğü takibi

[17] [atama: kriptografik işletimler listesi]
[18] [atama: kriptografik algoritma]
[19] [atama: kriptografik şifre boyutları]
[20] [atama: standartlar listesi]
[21] [atama: kriptografik işletimler listesi]
[22] [atama: kriptografik algoritma]
[23] [atama: kriptografik şifre boyutları]
[24] [atama: standartlar listesi]
[25] [atama: kullanıcıların tipi]
[26] [atama: bağlantı tipi]
[27] [atama: TSF verisinin tipleri listesi]
[28] [atama: kullanıcı verisi tiplerinin listesi]

Bağımlılıklar: Bağımlılık yoktur.

FDP_SDI.2.1 TSF, TSF tarafından tüm nesneler üzerinde [atama: bütünlük hataları][29] için kontrol edilen kapsayıcılarda depolanan kullanıcı verilerini, aşağıdaki özniteliklere dayalı olarak takip edecektir: *tüm uygulama verisi için*[30].

FDP_SDI.2.2 Veri bütünlük hatasının tespit edilmesi üzerine TSF [atama: yapılacak eylem][31] gerçekleştirecektir.

FDP_ITT.3 Bütünlük takibi

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: [FDP_ACC.1 Altküme erişim kontrolü, veya

FDP_IFC.1 FDP_ACC.1/PAP tarafından yerine getirilen Altküme bilgi akışı kontrolü]

FDP_ITT.1 FDP_ITT.1 tarafından yerine getirilen Temel dahili aktarım koruması

FDP_ITT.3.1 TSF, aşağıdaki hatalar için DH'nin fiziksel olarak ayrı kısımları arasında aktarımı yapılan kullanıcı verisini takip etmek için *Dahili Veri Erişimi Politikasını*[32] yürürlüğe koyacaktır: [atama: bütünlük hataları][33].

FDP_ITT.3.2 Bir veri bütünlüğü hatasının tespit edilmesi üzerine, TSF [atama: bütünlük hatası üzerine yapılacak eylemi belirle][34] gerçekleştirecektir.

FPT_TST.1 TSF testi

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_TST.1.1 TSF, *CPU İşletimi ve Rastgele Sayı Üretimi*[36] işleminin doğru çalışmasını kanıtlamak için, kendi kendine bir takım testler [seçim: ilk başlangıç esnasında, periyodik olarak normal işletim esnasında, yetkili kullanıcının talebiyle, şu koşullarda [atama: öz testlerin yapılacağı koşullar]][35].

FPT_TST.1.2 TSF yetkili kullanıcılara *TSF Verisinin*[37] bütünlüğünü doğrulama yetisi sağlayacaktır.

FPT_TST.1.3 TSF yetkili kullanıcılara *TSF'nin*[38] bütünlüğünü doğrulama yetisi sağlayacaktır.

[29] [atama: bütünlük hataları]
[30] [atama: kullanıcı verisi öznitelikleri]
[31] [atama: yapılacak eylem]
[32] [atama: erişim kontrolü FGG(leri) ve/veya bilgi akışı kontrolü FGG(leri)]
[33] [atama: bütünlük hataları]
[34] [atama: bütünlük hatası üzerine yapılacak eylemi belirle]
[35] [seçim: ilk başlangıç esnasında, periyodik olarak normal işletim esnasında, yetkili kullanıcının talebiyle, şu koşullarda [atama: öz testlerin yapılacağı koşullar]]
[36] [seçim: [atama: TSF'nin parçası], TSF]
[37] [seçim: [atama: TSF verilerinin parçaları], TSF verisi]
[38] [seçim: [atama TSF'nin parçaları], TSF]

6.1.3 FİZİKSEL SALDIRILARA KARŞI EK KORUMA

Bellek ve veri yolu şifrelemesi ve ayrıca hata tespiti, saldırganın bu şifreleme ve hata tespiti mekanizmalarına saldırabileceği için fiziksel saldırılara karşı yeterli değildir; bu nedenle ek fiziksel koruma gereklidir.

İlk olarak FPT_PHP.3, TSF'nin korunması için gereklidir.

FPT_PHP.3 Fiziksel saldırıya karşı direnç

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_PHP.3.1 TSF, [atama: TSF cihazları/öğeleri][40] üzerindeki *fiziksel sonda ve manipülasyona*[39], FGG'lerin her zaman geçerli olmasıyla otomatik olarak yanıt vererek karşı koyacaktır.

FPT_PHP.2 Fiziksel saldırının bildirimi

Hiyerarşi: FPT_PHP.1 Fiziksel saldırının pasif tespiti

Bağımlılıklar: FMT_MOF.1 Güvenlik işlevlerinin yönetimi davranışı yerine getirilmemiştir ancak gerekçelendirilmiştir.

FPT_PHP.2.1 TSF, TSF'yi bozabilecek fiziksel müdahalenin açık şekilde tespitini sağlayacaktır.

FPT_PHP.2.2 TSF, fiziksel müdahalenin TSF'nin cihazlarıyla mı yoksa TSF'nin öğeleriyle mi ilgili olduğunu belirleme yetisini sağlayacaktır.

FPT_PHP.2.3 [atama: aktif tespitin gerekli olduğu TSF cihazları/öğeleri listesi][41] için TSF, cihaz ve öğeleri takip edecek ve TSF cihazları veya TSF öğeleriyle ilgili fiziksel müdahale olduğunda *Tümleşik OS'ye*[42] bildirim yapacaktır.

Düzeltme: Yönetim tespiti fonksiyonelliği kapsamı (cihazlar/öğeler), herhangi bir cihaz veya öğe FPT_PHP.2.3 içinde seçildiyse ve bu nedenle bunun tespiti DH'nin tüm ömrü boyunca aktif olacağı için gerekli değildir. Ayrıca, bildirim yapılan varlık DH'nin ömrü boyunca Tümleşik OS olacaktır ve başka bildirim yapılan varlık olmayacaktır.

6.1.4 ORTAMSAL STRESTEN KORUMA

FPT_FLS.1 Güvenli durumun korunması aksaması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_FLS.1.1 TSF, aşağıdaki aksamalar ortaya çıktığında güvenli bir durumu koruyacaktır: *tolere edilemeyecek işletim koşullarına maruz kalmak*[43].

[39] [atama: fiziksel müdahale senaryoları]
[40] [atama: TSF cihazları/öğeleri listesi]
[41] [atama: aktif tespitin gerekli olduğu TSF cihazları/öğeleri listesi]
[42] [atama: atanmış bir kullanıcı veya rol]

6.1.5TEST İŞLEVLERİNİN İSTİSMARI

FMT_MOF.1/Test Güvenlik fonksiyonları davranışının yönetimi

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 FMT_SMR.1 tarafından yerine getirilen Güvenlik rolleri

FMT_SMF.1 FMT_SMF.1 tarafından yerine getirilen Yönetim Fonksiyonları Spesifikasyonu

FMT_MOF.1.1 TSF, *Üreticinin*[46] *üretim test fonksiyonlarını*[45] *devreden çıkarma*[44] yetisini kısıtlayacaktır.

Düzeltme: Test fonksiyonları devreden çıkarıldığı zaman, TSF test fonksiyonlarını geri dönülemez ve kalıcı şekilde devreden çıkarmalıdır; bu sayede tümleşik OS tarafından DH'nin kullanımı esnasında istismar edilmeleri mümkün olmayacaktır.

6.1.6 IC EŞSİZ TANILAMA VERİSİ

FMT_MTD.1/ID TSF Verisinin yönetimi - Tanılama

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 FMT_SMR.1 tarafından yerine getirilen Güvenlik rolleri

FMT_SMF.1 FMT_SMF.1 tarafından yerine getirilen, Yönetim Fonksiyonları Spesifikasyonu

FMT_MTD.1.1 TSF, *Üreticinin*[49], *IC Tanılama Verisini*[48] *bir kez yazma*[47] yetisini kısıtlayacaktır.

6.1.7RASTGELE SAYI ÜRETİMİ

FCS_RND.1 Rastgele sayılar için kalite ölçevi

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FCS_RND.1.1 TSF, [atama: tanımlanmış bir kalite ölçevini][50] karşılayacak rastgele sayıların üretilmesi için bir mekanizma sağlayacaktır.

---

[43] [atama: TSF içindeki aksamaların tiplerinin listesi]
[44] [seçim: davranışını belirle, devreden çıkar, devreye sok, davranışını değiştir]
[45] [atama: işlevlerin listesi]
[46] [atama: yetkili tanılanmış roller]
[47] [seçim: varsayılanı_değiştir, sorgu, değiştir, sil, temizle, [atama: diğer işlemler]]
[48] [atama: TSF verisi listesi]
[49] [atama: yetkili tanılanmış roller]
[50] [atama: tanımlanmış bir kalite ölçevi]

6.1.8 FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN EK FGG'LER

FIA_AFL.1 Doğrulama aksaması muamelesi

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FIA_UAU.1 FIA_UAU.1 tarafından yerine getirilen Doğrulama zamanlaması

FIA_AFL.1.1 TSF, *Flaş Yükleyici Doğrulama*[52] ile ilgili bir başarısız yetkilendirme girişimi olduğu zaman, [seçim: [atama: pozitif tamsayı] bir yönetici ayarlanabilir pozitif tamsayı [atama: kabul edilebilir değerler aralığı]][51] tespit yapacaktır.

FIA_AFL.1.2 Başarısız doğrulama girişimlerinin tanımlanmış sayısı [seçim: karşıladı, aştı][53] olduğu zaman, TSF [atama: eylemler listesi][54] yapacaktır.

FIA_UAU.1 Doğrulamanın zamanlaması

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FIA_UID.1 FIA_UID.1 tarafından yerine getirilen Tanılama zamanlaması

FIA_UAU.1.1 TSF, kullanıcının doğrulanmasın önce yerine getirilmek üzere kullanıcı adına *IC Tanılama verisinin yazılışı ve Test İşlevlerinin devreden çıkarılmasına*[55] izin verecektir.

FIA_UAU.1.2 TSF, o kullanıcı adına herhangi bir diğer TSF-aracılı eylemlere izin vermeden önce her bir kullanıcının başarılı şekilde doğrulanmasını gerektirecektir.

FIA_UAU.5 Çoklu doğrulama mekanizmaları

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FIA_UAU.5.1 TSF, kullanıcı doğrulamasını desteklemek için *Flaş Yükleyici Doğrulama Mekanizmasını*[56] sağlayacaktır.

FIA_UAU.5.2 TSF, herhangi bir kullanıcının iddia edilen kimliğini, *Kart Yayınlayıcı veya Üreticiyi doğrulayan Flaş Yükleyici Doğrulama Mekanizmasına*[57] göre doğrulayacaktır.

FIA_UID.1 Tanılamanın zamanlaması

[51] [seçim: [atama: pozitif tamsayı sayısı], [atama: kabul edilebilir değerler aralığı] içinde yönetici tarafından ayarlanabilir bir pozitif tamsayı]
[52] [atama: doğrulama olaylarının listesi]
[53] [seçim: karşıladı, aştı]
[54] [atama: eylemler listesi]
[55] [atama: TSF aracılı eylemler listesi]
[56] [atama: çoklu doğrulama mekanizmaları listesi]
[57] [atama: çoklu doğrulama mekanizmalarının doğrulamayı nasıl sağladığını açıklayan kurallar]

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FIA_UID.1.1 TSF, kullanıcının tanılanmasından önce kullanıcı adına *IC Tanılama veri yazımı ve Test ;işlevlerinin devreden çıkarılmasına*[58] izin verecektir.

FIA_UID.1.2 TSF, o kullanıcı adına herhangi bir diğer TSF-aracılı eylemlere izin vermeden önce her bir kullanıcının başarılı şekilde doğrulanmasını gerektirecektir.

FMT_MTD.1/ES TSF verisinin Yönetimi – Tümleşik OS

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 FMT_SMR.1 tarafından yerine getirilen Güvenlik rolleri

FMT_SMF.1 FMT_SMF.1 tarafından yerine getirilen Yönetim Fonksiyonları Spesifikasyonu

FMT_MTD.1.1 TSF, *Tümleşik OS'nin*[60], *Üreticiye ve Kart Yayınlayıcıya*[61] *yazılmasını*[59] kısıtlayacaktır.

FMT_MOF.1/FL Güvenlik işlevleri davranışının yönetimi – Flaş Yükleyici

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 FMT_SMR.1 tarafından yerine getirilen Güvenlik rolleri

FMT_SMF.1 FMT_SMF.1 tarafından yerine getirilen Yönetim Fonksiyonları Spesifikasyonu

FMT_MOF.1.1 TSF, *Üreticinin ve Kart Yayınlayıcının*[64], *Tümleşik OS Yükleme*[63] işlevlerinin *devreden çıkarılması*[62] yetisini kısıtlayacaktır.

6.1.9 GÜVENLİK YÖNETİMİ FONKSİYONLARI VE ROLLERİ

FMT_SMF.1 Yönetim Fonksiyonları Spesifikasyonu

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

[58] [atama: TSF-aracılı eylemlerin listesi]
[59] [seçim: varsayılanı_değiştir, sorgula, değiştir, sil, temizle, [atama: diğer işlemler]]
[60] [atama: TSF verisi listesi]
[61] [atama: yetkili tanılanmış roller]
[62] [seçim: davranışını belirle, devreden çıkar, devreye sok, davranışını değiştir]
[63] [atama: fonksiyonların listesi]
[64] [atama: yetkili tanılanmış roller]

FMT_SMF.1.1 TSF, aşağıdaki yönetim fonksiyonlarını yapabilecektir:

- *Üretim test fonksiyonlarının devreden çıkarılması*
- *IC tanılama bilgisini bir kez yazma*
- *Tümleşik OS Yükleme*
- *Tümleşik OS Yükleme Kilitleme*
- [atama: TSF tarafından sağlanacak yönetim fonksiyonlarının listesi][65].

Uygulama Notu:

Tümleşik OS Yükleme ve Tümleşik OS Yükleme Kilitleme, Flaş Yükleyici Konfigürasyonu için geçerlidir. ROM tabanlı konfigürasyon için mevcut değillerdir.

FMT_SMR.1 Güvenlik rolleri

Hiyerarşi: Başka bileşen yoktur.

Bağımlılıklar: FIA_UID.1 Tanılama zamanlaması yerine getirilmemiş ancak gerekçelendirilmiştir.

FMT_SMR.1.1 TSF şu rolleri idame ettirecektir:

- *Üretici*
- *Kart Yayınlayıcı*
- *Tümleşik OS*
- [atama: yetkili tanılanmış rollerin listesi][66].

FMT_SMR.1.2 TSF, kullanıcıları rollerle ilişkilendirebilecektir.

Uygulama Notu:

Kart Yayınlayıcı rolü, tümleşik OS Kart Yayınlayıcı tarafından yüklendiyse sadece Flaş Yükleyici konfigürasyonu için mevcuttur; aksi takdirde bu rol mevcut değildir.

[65] [atama: TSF tarafından sağlanacak yönetim fonksiyonlarının listesi]
[66] [atama: yetkili tanılanmış roller]

6.2 ASSURANCE REQUIREMENTS

DH'nin değerlendirilmesi için gerekli olan DH Güvenlik Garanti Gereksinimleri, Değerlendirme Garanti Seviyesi 5'ten (EAL5) alınan ve aşağıdaki bileşenleri de alarak arttırılan gereksinimlerdir:

- ALC_DVS.2 Güvenlik önlemlerinin yeterliliği
- AVA_VAN.5. Gelişmiş düzenli korunmasızlık analizi

6.3 GÜVENLİK GEREKSİNİMLERİ RASYONELİ

6.3.1 FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ İÇİN RASYONEL

Aşağıdaki tablo, fonksiyonel güvenlik gereksinimlerin kapsamı için genel bir bakış sağlamaktadır.

No:	Güvenlik Hedefi	Fonksiyonel Güvenlik Gereksinimleri
1.	OT.Veri Erişim Kontrolü	FDP_ACC.2, FDP_ACF.1, FCS_CKM.1/DP, FCS_CKM.4, FCS_COP.1/DP, FPT_PHP.3, FPT_PHP.2
2.	OT.Veri Bütünlüğü	FDP_SDI.2, FPT_TST.1, FPT_PHP.3, FPT_PHP.2 **Artı OT.Veri Erişim Kontrolü için FGG'ler** FDP_ACC.2, FDP_ACF.1, FCS_CKM.1/DP, FCS_CKM.4, FCS_COP.1/DP
3.	OT.Dahili DH Aktarım Gizliliği Koruması	FDP_ITT.1 FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP FPT_PHP.3, FPT_PHP.2
4.	OT.Dahili DH Aktarım Bütünlüğü Koruması	FDP_ITT.3 FPT_PHP.3, FPT_PHP.2 **Artı OT. Dahili DH Aktarım Gizliliği Koruması için FGG'ler** FDP_ITT.1 FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP
5.	OT.CPU_İşletim Koruması	FPT_TST.1
6.	OT.Rastgele Sayı Üretimi Koruması	FPT_TST.1
7.	OT.Yan Kanallı Koruma	FPT_SCP.1
8.	OT.Ortamsal Stres Koruması	FPT_FLS.1
9.	OT.Test Fonksiyonları Devreden Çıkarma Mekanizması	FPT_MOF.1/Test, FMT_SMF.1, FMT_SMR.1
10.	OT.Eşsiz ID Depolama	FMT_MTD.1/ID, FMT_SMF.1, FMT_SMR.1
11.	OT.Rastgele Sayı Üretimi	FCS_RND.1

Tablo 3: Fonksiyonel Güvenlik Gereksinimleri Rasyoneli

FLAŞ YÜKLEME KONFİGÜRASYONU İÇİN EK RASYONEL

12.	OT.Flaş Yükleyici İşlevselliği	FPT_MTD.1/ES, FMT_SMF.1, FMT_SMR.1
13.	OT.Flaş Yükleyici Yetkisi	FIA_AFL.1, FIA_UAU.1, FIA_UAU.5, FIA_UID.1
14.	OT.Flaş Yükleyici Devreden Çıkarma Mekanizması	FPT_MOF.1/FL, FMT_SMF.1, FMT_SMR.1

Tablo 4: Fonksiyonel Güvenlik Gereksinimleri Rasyoneli

OT.Veri Erişim Kontrolü

FDP_ACC.2 ve FDP_ACF.1, saldırganı engellerken tümleşik OS'ye erişim sağlar. Bu, veriyi şifreleyerek depolama ve FCS_CKM.1/DP, FCS_CKM.4 ve FCS_COP.1/DP'nin desteğiyle şifreyi çözme vasıtasıyla yerine getirilir. FPT_PHP.3 ve FPT_PHP.2, fiziksel saldırılara karşı ek koruma sağlar.

OT.Veri Bütünlüğü

FDP_SDI.2 ve FPT_TST.1, verinin bütünlüğünü takip eder ve GH yazarı tarafından belirlenmiş olan eylemleri gerçekleştirir. OT.Veri Erişim Kontrolünü kapsayan FGG'ler, şifreli veriye makul değişiklikleri imkansız hale getirmek için bu hedef için de geçerlidir.

OT.Dahili DH Aktarım Gizliliği Koruması

FDP_ITT.1, veri DH'nin dahili parçaları arasında aktarımdayken koruma sağlar. Koruma, dahili veri trafiğinin şifrelenmesiyle yerine getirilir; şifreleme ve şifre çözme işlemleri, FCS_CKM.1/TP, FCS_CKM.4, FCS_COP.1/TP gereksinimleri tarafından yapılır. FPT_PHP.3 ve FPT_PHP.2, fiziksel saldırılara karşı ek koruma sağlar.

OT.Dahili DH Aktarım Bütünlüğü Koruması

FDP_ITT.3, aktarılan verinin bütünlüğünü takip eder ve GH yazarı tarafından belirlenmiş olan eylemleri yerine getirir. FPT_PHP.3 ve FPT_PHP.2, fiziksel saldırılara karşı ek koruma sağlar. OT. Dahili DH Aktarım Gizliliği Koruması'nı kapsayan FGG'ler, şifreli veri üzerinde makul değişiklikleri imkansız hale getirecek şekilde bu hedef için de geçerlidir.

OT.CPU İşletim Koruması

FPT_TST.1'ye, CPU'nun doğru çalışması testi de dahildir ve bu sayede OT.CPU İşletim Korumasını da kapsar.

OT.Rastgele Sayı Üretimi Koruması

FPT_TST.1'ye, Rastgele Sayı Üretimi İşlevselliğinin doğru çalışması testi de dahildir ve bu sayede OT.Rastgele Sayı Üretimi Korumasını da kapsar.

OT.Yan Kanallı Koruma

FPT_SCP.1, DH'yi yan kanallı saldırılara karşı korur.

OT.Ortamsal Stres Koruması

FPT_FLS.1, DH'nin başa çıkamayacağı ortamsal stresle karşılaşması durumunda güvenli durumun muhafaza edilmesini gerektirmektedir.

OT.Eşsiz ID Depolama

FMT_MTD.1, üreticinin IC Tanılama verisini yazması işlevini sağlar. Bu sayede OT.Eşsiz ID Depolama da kapsanmış olur.

OT.Rastgele Sayı Üretimi

FCS_RND.1, OT.Rastgele Sayı Üretimi'nin beyan ettiği rastgele sayı üretimi işlevselliğini sağlar.

OT.Test Fonksiyonları Devreden Çıkarma Mekanizması

FMT_MOF.1/FL, test işlevselliğinin geri dönülemez şekilde devreden çıkarılması işlevselliğini sağlar. FMT_SMF.1 ve FMT_SMR.1, bu işlevselliği ve ilgili rolleri tanımlar.

FLAŞ YÜKLEYİCİ KONFİGÜRASYONU İÇİN EK RASYONEL

OT.Flaş Yükleyici İşlevselliği

FPT_MTD.1/ES, tümleşik işletim sistemi yüklemi işlevini sağlar. FMT_SMF.1 ve FMT_SMR.1, bu işlevselliği ve ilgili rolleri tanımlar.

OT.Flaş Yükleyici Yetkilendirme

FIA_UAU.5, bir Flaş Yükleyici Yetkilendirme mekanizmasının mevcut olmasını gerektirir ve FIA_UAU.1 ve FIA_UID.1, Flaş Yükleyici işleminin, kullanıcının tanılama ve yetkilendirilmesinde önce yapılmasını gerektirir. Son olarak FIA_AFL.1, Flaş Yükleyici yetkilendirme mekanizmalarını hileli yetkilendirme girişimlerine karşı korur.

OT.Flaş Yükleyici Devreden Çıkarma Mekanizması

FMT_MOF.1/FL, flaş yükleyici mekanizmasının geri dönülemez şekilde devreden çıkarılması işlevselliğini sağlar. FMT_SMF.1 ve FMT_SMR.1, bu işlevselliği ve ilgili rolleri tanımlar.

6.3.2 FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ İÇİN BAĞIMLILIKLAR

FGG	Bağımlılıklar	Bağımlılıkların Desteği
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1/PAP tarafından yapılır
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/PAP tarafından yapılır gerekçelendirilmiştir (bakınız gerekçe.1)
FDP_ITT.1	FDP_ACC.1 Altküme erişim kontrolü, veya FDP_IFC.1 Altküme bilgi akışı kontrolü	FDP_ACC.1/PAP tarafından yapılır
FCS_CKM.1/PAP	[FCS_CKM.2 Kriptografik şifre dağıtımı, veya FCS_COP.1 Kriptografik işlem] FCS_CKM.4 Kriptografik şifre imhası	FCS_COP.1 tarafından yapılır FCS_CKM.4 tarafından yapılır
FCS_CKM.4	[FDP_ITC.1 Kullanıcı verisinin güvenlik öznitelikleri olmadan alınması veya FDP_ITC.2 Kullanıcı verisinin güvenlik öznitelikleriyle alınması, veya FCS_CKM.1 Kriptografik şifre üretimi]	FCS_CKM.1 tarafından yapılır
FCS_COP.1/PAP	[FDP_ITC.1 Kullanıcı verisinin güvenlik öznitelikleri olmadan alınması veya FDP_ITC.2 Kullanıcı verisinin güvenlik öznitelikleriyle alınması, veya FCS_CKM.1 Kriptografik şifre üretimi] FCS_CKM.4 Kriptografik şifre imhası	FCS_CKM.1 tarafından yapılır FCS_CKM.4 tarafından yapılır
FDP_SDI.2	Yok	---
FDP_ITT.3	[FDP_ACC.1 Altküme erişim kontrolü, veya FDP_IFC.1 Altküme bilgi akışı kontrolü] FDP_ITT.1 Temel dahili aktarım koruması	FDP_ACC.1/PAP tarafından yapılır FDP_ITT.1 tarafından yapılır
FPT_TST.1	Yok	---
FPT_PHP.3	Yok	---
FPT_PHP.2	FMT_MOF.1 Güvenlik fonksiyonları davranışının yönetimi	Yerine getirilmemiştir ancak gerekçelendirilmiştir
FPT_FLS.1	Yok	---
FMT_MOF.1/Test	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim Fonksiyonlarının Yönetimi	FMT_SMR.1 tarafından yapılır FMT_SMF.1 tarafından yapılır

FMT_MTD.1/Tanılama	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim Fonksiyonlarının Yönetimi	FMT_SMR.1 tarafından yapılır FMT_SMF.1 tarafından yapılır
FCS_RND.1	Yok	---
FPT_SCP.1	Yok	----
FMT_SMF.1	Yok	---
FMT_SMR.1	FIA_UID.1	FIA_UID.1 tarafından yapılır

Tablo 5: FGG'ler için Bağımlılıklar

Gerekçe 1: FPT_ACF.1, tüm veriler için geçerlidir. Bu yüzden güvenlik özniteliği yönetimi gerekli değildir.
Gerekçe 2: Yönetim tespit işlevsellik kapsamı (cihazlar/öğeler), herhangi bir cihaz veya öğe FPT_PHP.2.3 içinde seçildiyse tespiti DH'nin ömrü boyunca aktif olacağından dolayı gerekli değildir. Ayrıca, bildirim yapılan öğe DH'nin ömrü boyunca Tümleşik OS olacaktır ve başka bir bildirim yapılan varlık olmayacaktır.

FLAŞ YÜKLEYİCİ İÇİN EKLER

FGG	**Bağımlılıklar**	**Bağımlılıkların Desteği**
FIA_AFL.1	FIA_UAU.1 Doğrulamanın Zamanlaması	FIA_UAU.1 tarafından yapılır
FIA_UAU.1	FIA_UID.1 Tanılamanın zamanlaması	FIA_UID.1 tarafından yapılır
FIA_UAU.5	Yok	----
FIA_UID.1	Yok	----
FMT_MTD.1/ES	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim Fonksiyonlarının Yönetimi	FMT_SMR.1 tarafından yapılır FMT_SMF.1 tarafından yapılır
FMT_MOF.1/FL	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim Fonksiyonlarının Yönetimi	FMT_SMR.1 tarafından yapılır FMT_SMF.1 tarafından yapılır

Tablo 6: Flaş Yükleyicinin Ek FGG'leri için Bağımlılıklar

6.3.3GGG'LER İÇİN RASYONEL VE BAĞIMLILIKLAR

Bu KP dahilindeki DH, YÜKSEK saldırı potansiyeline sahip saldırganlara karşı direnmeyi amaçlamaktadır; bu yüzden, fonksiyonel gereksinimlerin yanı sıra, mimari sağlamlık ve iyi tanımlanmış ve test edilmiş dahili parçalar gibi güvenlik gereksinimleri de önemlidir. EAL5 paketi, yarı resmi tasarım açıklamaları, daha iyi yapılandırılmış (ve bu sayede analiz edilebilir) bir mimari, EAL4'ün gerektirmediği dahili odaklı test unsurlarını gerektirmektedir. Bu yüzden, DH ve EAL5 için olan gereksinimler eşleşmektedir. Ters mühendislik de DH için önemli bir tehdit olduğundan ve Geliştirme Ortamından beklenen garanti yüksek olduğundan; ALC_DVS.2 eklenmiştir. Son olarak, YÜKSEK saldırı potansiyeline sahip saldırganlara karşı koymak için, AVA_VAN.5 eklenmiştir.

EAL5 – EAL4 Farklılıkları

EAL4	**EAL5**
ADV_FSP.4	ADV_FSP.5
---	ADV_INT.2
ADV_TDS.3	ADV_TDS.4
ALC_CMS.4	ALC_CMS.5
ALC_TAT.1	ALC_TAT.2
ATE_DPT.1	ATE_DPT.3
AVA_VAN.3	AVA_VAN.4

Tablo 7: EAL4 ve EAL5 arasındaki Farklar

Eklenmiş GGG'ler için bağımlılıklar:

GGG	**Bağımlılıklar**	**Bağımlılıkların Desteği**
ALC_DVS.2	Yok	---
AVA_VAN.5	ADV_ARC.1 Güvenlik mimarisi açıklaması ADV_FSP.4 Tüm işlevsel spesifikasyon ADV_TDS.3 Temel modüler tasarım ADV_IMP.1 DH'nin uygulama temsili AGD_OPE.1 İşletim kullanım kılavuzu AGD_PRE.1 Hazırlık prosedürleri ATE_DPT.1 Test etme: temel tasarım	EAL5'e dahil edilmiştir

Tablo 8: Eklenmiş GGG'ler için Bağımlılıklar

6.3.4 GÜVENLİK GEREKSİNİMLERİ – KARŞILIKLI DESTEK VE İÇ TUTARLILIK

Yürürlükteki KP, YÜKSEK saldırı potansiyeline sahip saldırganlara karşı koymayı amaçlamaktadır. Hem FGG'ler hem de GGG'ler, bu amaca ulaşmak için seçilmiştir. Her iki gereksinim tipinin fonksiyonel gereksinimler ve garanti gereksinimleri) rasyonelleri verilmiş ve bunların bağımlılık analizleri yapılmıştır; bir tutarsızlık mevcut değildir. FGG'ler ve GGG'ler birbirlerini dahili olarak desteklemektedir.

FGG'lerin ve GGG'lerin birbirlerine desteği, GGG'lerin gerekli işlevsellik için yeterli garanti vermeye yetkin olması şeklinde sağlanmaktadır.

REFERANSLAR

[1] Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 1: Giriş ve Genel Model; CCMB-2012-09-001, Sürüm 3.1, Revizyon 4, Eylül 2012

[2] Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 2: Fonksiyonel Güvenlik Gereksinimleri; CCMB-2012-09-002, Sürüm 3.1, Revizyon 4, Eylül 2012

[3] Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Kriterler, Kısım 3: Güvenlik Garanti Gereksinimleri; CCMB-2012-09-003, Sürüm 3.1, Revizyon 1, Eylül 2012

[4] Bilişim Teknolojisi Güvenlik Değerlendirmesi için Ortak Metodoloji (CEM), Değerlendirme Metodolojisi; CCMB-2012-09-004, Sürüm 3.1, Revizyon 4, Eylül 2012