Web Uygulamaları Koruma Profili

SÜRÜM 1.0

TÜRK STANDARDLARI ENSTİTÜSÜ

KASIM 2013

İÇİNDEKİLER

TANIMLAR VE KISALTMALAR

Belge: Herhangi bir bireysel veya kurumsal fonksiyonun yerine getirilmesi için alınmış ya da fonksiyonun sonucunda üretilmiş, içerik, ilişki ve formatı ile ait olduğu fonksiyon için delil teşkil eden kayıtlı bilgi.

BT: Bilgi Teknolojileri

Değerlendirme Garanti Seviyesi (Evaluation Assurance Level, EAL): Ortak Kriterler standardının Bölüm 3'de verilen garanti bileşenlerinden oluşan ve 1-7 aralığında önceden belirlenmiş değerler alan güvenlik seviyesi paketidir.

Değerlendirme Hedefi (Target of Evaluation, TOE): Ortak Kriterler güvenlik değerlendirmesine konu olan Bilgi Teknolojileri ürünü ya da sistemidir.

Doküman: Kurumsal faaliyetlerin yerine getirilmesinde üretilen ya da toplanan, henüz belge vasfı kazanmamış her türlü bilgi.

DGF: Değerlendirme Hedefi Güvenlik Fonksiyonları

DGS: Değerlendirme Garanti Seviyesi

FGG : Fonksiyonel Güvenlik Gereksinimleri

Elektronik İmza (e-İmza): Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir.

EKP: Erişim Kontrol Politikası

Güvenlik Fonksiyon Politikası (GFP): Değerlendirme Hedefinin Güvenlik Fonksiyonları (DGF) tarafından zorunlu kılınan güvenlik davranışlarını tanımlayan kurallardır.

Güvenlik Hedefi (GH): Bir ürün geliştiricinin, ürünün güvenlik özelliklerini kanıtlamak için kullandığı güvenlik değerlendirme kriterleri dokümanıdır.

Kurumsal Güvenlik Politikaları: Gerçek ya da sanal bir kuruluş tarafından, şimdi ve/veya gelecekte uygulamaya alınacak olan güvenlik kuralları, prosedürleri ya da kurallar dizisidir.

Koruma Profili (KP): Bir DH türü için, uygulamadan bağımsız güvenlik ihtiyaçlarının tanımlandığı dokümandır.

Kurumsal Güvenlik Politikaları (KGP): Bir organizasyon tarafından uygulanması zorunlu kılınan, güvenlik kuralları, prosedürler ya da operasyonlardır.

LAN (Local Area Network): Yerel Alan Ağı

Ortak Kriterler (OK): Bilgi teknolojileri ürünlerinin güvenlik seviyelerinin tespit edilmesi ve bağımsız laboratuarlarda test edilebilmesi için geliştirilmiş olan, temelini Amerika'daki TCSEC (Telecommunication Security) ve Avrupadaki ITSEC (IT Security) standartlarından alan ve Uluslararası Standartlar Organizasyonu'nun (ISO) 1999 yılında Uluslararası Bilgi Teknolojileri Güvenlik Değerlendirme Standardı olarak kabul ettiği (ISO 15408) BT ürün güvenliği standardıdır.

Nitelikli Elektronik Sertifika: 5070 sayılı Elektronik İmza Kanununa göre oluşturulmuş, güvenli elektronik imza sertifikasıdır.

Tehdit: Değerlendirme Hedefi üzerinde olumsuz etki yapan davranışlardır.

Varlıklar: Değerlendirme Hedefi'nin sahip olduğu varlıklardır.

WAN (Wide Area Networ): Geniş Alan Ağı

Yetkilendirilmiş Yönetici : Güvenlik Fonksiyonel Gereksinimleri uyarınca, Değerlendirme Hedefi üzerinde yönetimsel işlemleri gerçekleştirebilecek yetkili kullanıcıdır.

Yetkili Kullanıcı: Güvenlik Fonksiyonel Gereksinimleri uyarınca, Değerlendirme Hedefi üzerinde işlemleri gerçekleştirebilecek kullanıcıdır.

1. KORUMA PROFİLİNE GİRİŞ

1.1. KORUMA PROFİLİ REFERANSI

Aşağıdaki tabloda, koruma profiline ait referans bilgileri yer almaktadır.

Belge Sürümü	1.0
Yayınlanma Tarihi	
Geliştirici	TÜRK STANDARDLARI ENSTİTÜSÜ
Uyum Sağlanan EAL	EAL 2+
Anahtar Kelimeler	Web uygulamaları, internet, intranet, internet tabanlı uygulamalar, güvenli web.

1.2. AMAÇ VE KAPSAM

Web uygulamalarına yönelik genel amaçlı olarak hazırlanmış olan bu koruma profilinin oluşturulma amacı, kamu kurumları ve özel sektörde kullanılan web uygulamalarına yönelik asgari güvenlik gereksinimlerinin tanımlanmasıdır. İnternetin yaygınlaşmaya başladığı ilk dönemlerde statik içeriğe sahip web siteleri, kuruluşlarca kullanılmaya başlanmıştır. Gerek internet altyapısının kapasite olarak artması, gerekse web teknolojilerindeki ve programlama dillerindeki gelişmeler ve çeşitlilik, web sitelerinin yerlerini web uygulamalarına bırakmasına sebep olmuştur. İnteraktif olarak adlandırılabilecek ilk web siteleri, basit anlamda formlara sahip olup bu formların siteyi ziyaret edenlerce doldurulmasına imkân tanımaktaydı. Bu tür siteler, web uygulamalarının ilk örnekleri olarak görülebilir. Bu uygulamalar literatürde birer web uygulaması örneği olarak nitelenmekle birlikte bu koruma profili kapsamına girecek nitelikteki web uygulamalarının daha karmaşık yapıda olması beklenir.

Web uygulamalarında interaktif özellikler o denli artmıştır ki, günümüzde web uygulamalarıyla masaüstü uygulamaları arasındaki fark oldukça azalmıştır. İnteraktif özelliklerin artması, internetin tehditlere açık yapısıyla beraber düşünüldüğünde, üst düzey güvenlik önlemlerini zorunlu kılmaktadır. Kuruluşların söz konusu güvenlik önlemlerini etkin ve gerektiği şekilde almalarının temin edilmesi, ancak standartlara uyum ve ilgili sertifikasyonların faaliyete geçirilmesiyle mümkündür. Bu koruma profilinin yazılma amacı, genel amaçlı web uygulamalarına yönelik böylesi bir sertifikasyon mekanizmasında yol gösterici bir belgenin oluşturulması ihtiyacıdır.

Bu koruma profili, orta seviye güvenlik önlemlerini tamamıyla kapsamakla birlikte, uğraştırıcı nitelikte ve ancak üst düzey güvenlik ihtiyacında söz konusu olabilecek bazı güvenlik gereksinimlerini kapsam dışı bırakmaktadır. Bunun nedeni, dinamik yapıları sebebiyle uzun ve uğraştırıcı sertifikasyon süreçlerine uyum sağlayamayacak nitelikteki web uygulamalarının da kapsanabilmesi için sertifikasyon süresinin kısa tutulması ihtiyacıdır. EAL seviyesi seçiminde de aynı çekinceyle EAL seviyesi görece düşük bir seviye olarak belirlenmiştir.

Koruma profili genel amaçlı web uygulamalarına yönelik olarak hazırlanmıştır. Başka bir deyişle, tüm web uygulamalarında geçerli fonksiyonel özellikler ve bileşenler dikkate alınmış, bunun haricinde uygulamaların kendilerine özgü fonksiyonel özellik ve bileşenleri kapsam dışı bırakılmıştır. Bu koruma profilinin kapsamı dışında kalan, ancak güvenlik sertifikasyonundan geçirilmesi gerekli görülen güvenlik özellikleri veya bileşenler olabilir. Bu özellik ve bileşenlerin sertifikasyon mekanizmasına tabi tutulması isteniyorsa, bu iki alternatif yöntemle gerçekleştirilebilir; İlk alternatif, uygulamaya yönelik oluşturulacak Güvenlik Hedefi (ST) dokümanında, bu koruma profilinde kapsanmamış olan güvenlik özelliklerinin ve bileşenlerin kapsam dâhiline alınmasıdır. İkinci ve önerilen alternatif ise web uygulaması olarak nitelendirilebilecek ürün grupları için yazılacak koruma profillerinde bu koruma profiline atıf yapılmasıdır.

Literatürde bir uygulamanın web uygulaması olarak nitelenebilmesi için uygulamanın internet veya intranet üzerinden erişime açık olması gerekmektedir. Ancak internet ortamı ile intranet ortamının güvenlik tehditleri ve dolayısıyla güvenlik önlemleri büyük ölçüde farklılık arz etmektedir. Bu nedenle koruma profili yazılırken, uygulamanın internet üzerinden erişime açık olduğu varsayılmıştır. İntranet üzerinden erişime açık uygulamalar için de bu koruma profilinin uygulanması tavsiye edilmektedir. Öte yandan, bazı özelliklerin internet üzerinden sunulduğu, ancak genel itibariyle intranet üzerinden erişime izin veren uygulamalar da bulunmaktadır. Bu uygulamaların tamamının bu koruma profiline uyum sağlaması söz konusu olabileceği gibi, uygulamaların sadece internet üzerinden erişilebilen kısımlarının uyumu da düşünülebilir.

Bir web uygulamasının bu koruma profiline uygun olup olmadığı değerlendirilirken, web uygulamasının korumakla yükümlü olduğu verinin kritiklik ve gizlilik derecesi, veri kaybında, izinsiz değiştirilmesinde veya sızdırılmasında ortaya çıkacak maddi veya manevi zararın büyüklüğü gibi hususlar da hesaba katılmalıdır. Bir banka tarafından kullanılan yazılım altyapısı ile herhangi bir web uygulaması doğal olarak aynı kategoride değerlendirilemeyecektir. Bu nedenle, TOE'nin güvenliği sağlanmadığında ortaya çıkacak maddi kaybın veya prestij kaybının, koruma profiline uyum için harcanacak para, vakit ve emeğin mali karşılığından fazla olması durumunda bu koruma profiline uyum sağlanması tavsiye edilmektedir. Kamu bilişim sistemlerinde her durumda prestij kaybından ve/veya mali kayıptan söz edilememekle birlikte, güvenlik e-devlet uygulamalarının yaygınlaşmasında kilit öneme sahip konulardan birisidir.

1.3. DEĞERLENDİRME HEDEFİNE (TOE) GENEL BAKIŞ

Bu bölümde, koruma profilinin değerlendirme hedefi (TOE) açıklanmaktadır.

1.3.1. GİRİŞ

TOE, bir web uygulamasıdır. Web uygulaması, kullanıcıların internet veya yerel ağ (intranet) gibi bir ağ üzerinden erişim sağladıkları uygulamalara verilen genel bir isimdir. Ancak 1.2 no'lu "Amaç ve Kapsam" bölümünde de değinildiği üzere, uygulamanın internet üzerinden erişilebilir olduğu varsayılmıştır.

Bu koruma profili, tüm web uygulamalarını kapsayacak şekilde genel bir bakış açısıyla hazırlanmıştır. Bu nedenle koruma profili, sadece tüm web uygulamalarında ortak olarak bulunan güvenlik fonksiyonel özellikleri ve sistem bileşenleri dikkate alınarak hazırlanmıştır. Belirli bir konuda özelleşmiş web uygulamaları (e-ticaret uygulamaları, e-devlet uygulamaları gibi) bu koruma profiline atıfta bulunabilir, ancak bu uygulamaların kendilerine has olan güvenlik fonksiyonel özelliklerinin ayrı bir koruma profilinde ele alınması, genel hususlarda ise bu koruma profiline atıfta bulunması önerilmektedir.

1.3.2. DEĞERLENDİRME HEDEFİ TÜRÜ

TOE türü, "internet üzerinden erişilebilen, orta seviye güvenlik ihtiyacına sahip web uygulaması" dır.

1.3.3. ÇALIŞMA ORTAMI BİLEŞENLERİ

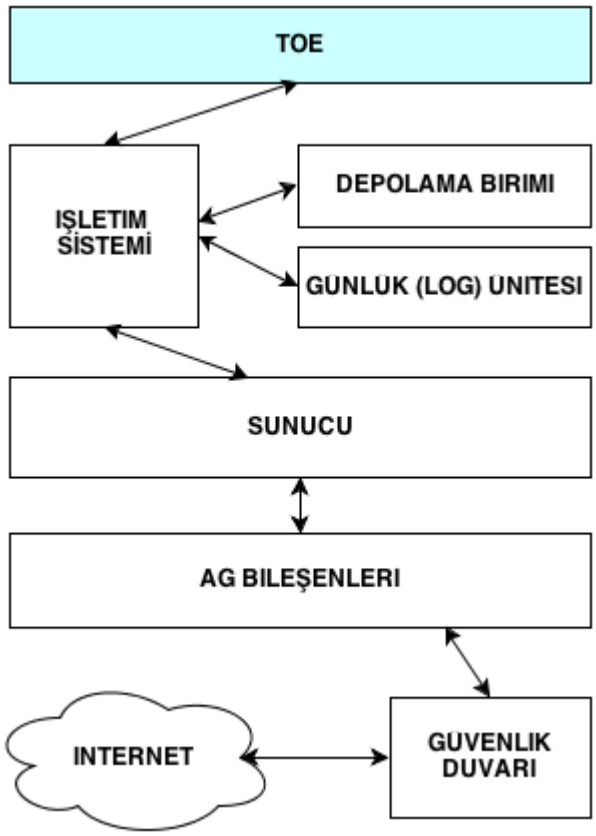
TOE, bir ağ üzerinde çalışması sebebiyle ağ bileşenleriyle etkileşim halindedir. TOE'nin üzerinde çalıştığı bir işletim sistemi, bu işletim sisteminin de üzerinde çalıştığı bir sunucu bulunmaktadır. TOE ayrıca kayıtların ve (varsa) dokümanların tutulduğu depolama birimleriyle etkileşim halindedir. Bunlara ek olarak TOE, günlük kayıtlarının tutulduğu bir günlük tutma ünitesiyle de etkileşim halindedir. Bu bileşenler aşağıda detaylı bir şekilde açıklanmaktadır.

1.4. DEĞERLENDİRME HEDEFİNİN DETAYLI AÇIKLANMASI

Bu bölümde, TOE daha ayrıntılı olarak açıklanacak, TOE'nin yazılımsal ve donanımsal çevre birimleri (çalışma ortamı) ile ana güvenlik ve fonksiyonel özellikleri ele alınacaktır.

1.4.1. YAZILIMSAL VE DONANIMSAL ÇEVRE BİRİMLERİ

Bu bölümde, TOE ile etkileşim halinde olan yazılımsal ve donanımsal çevre birimleri (çalışma ortamı) açıklanmaktadır. TOE'nin çalışma ortamıyla nasıl bir etkileşim içerisinde olduğu Şekil 1'de gösterilmektedir.



İşletim Sistemi: TOE, bir işletim sistemi üzerinde çalışmaktadır. TOE'nin depolama birimi, günlük (log) ünitesi ile sunucu ve ağ bileşenleri arasındaki iletişim işletim sistemi vasıtasıyla sağlanmaktadır.

Depolama Birimi: Uygulama kayıtları ve dokümanlar ayrı depolama birimlerinde tutulabileceği gibi, aynı depolama birimi üzerinde de tutulabilir. Söz konusu edilen her iki depolama birimi de TOE'nin çalıştığı sunucu üzerinde bulunabilir. Depolama birimlerinin TOE ile aynı sunucuyu paylaştığı bu alternatif de dikkate alınmıştır, çünkü basit seviyeli web uygulamaları için TOE ve depolama birimlerinin aynı sunucuyu paylaşmaları normal kabul edilebilir. Ancak depolama birimleri (örneğin veritabanı) ile TOE'nin farklı sunucular üzerinde çalışması, güvenlik açısından avantajlı olup kuvvetle önerilmektedir.

Günlük (Log) Ünitesi: Depolama ünitelerine benzer şekilde, günlük tutma ünitesi de TOE ile aynı sunucu üzerinde veya sisteme ait diğer kayıtların tutulduğu depolama birimi üzerinde tutulabilir.

Sunucu: İşletim sisteminin üzerinde çalıştığı donanım bileşenidir.

Ağ Bileşenleri: TOE, ağ bileşenleriyle etkileşim halindedir. Bu etkileşim, işletim sistemi ve sunucu aracılığıyla gerçekleştirilir.

Güvenlik Duvarı: TOE'nin internet erişimi, bir güvenlik duvarı tarafından denetlenmektedir.

1.4.2. ANA GÜVENLİK VE FONKSİYONEL ÖZELLİKLER

Kimlik Doğrulama ve Yetkilendirme: Özellikle TOE'nin internete açık bir ortamda bulunması sebebiyle, TOE'nin kimlik doğrulama ve yetkilendirme işlemlerini etkin bir şekilde yürütmesi gerekir. Kimlik doğrulama genellikle kullanıcı adı ve şifrenin doğrulanması yöntemiyle yapılır. Üst düzey güvenlik ihtiyacı bulunan web uygulamalarında iki aşamalı doğrulama adı verilen, kullanıcı adı ve şifreye ek olarak SMS doğrulaması, parola, mobil cihaz uygulaması aracılığıyla doğrulama, elektronik imza gibi ek doğrulama mekanizmaları da kullanılabilmektedir. Şifreler genellikle özet fonksiyonlarından geçirilerek tekrar aslında ulaşılamayacak şekilde saklanır. Ancak, özet bilgisinin SALT değişkeniyle birlikte kullanılması önerilen bir yöntemdir.

Denetim: TOE, sistemdeki varlıklar üzerindeki kullanıcı faaliyetlerinin, erişim kontrolü ve sistem yapılandırma değişikliklerinin kayıt altına alınabilmesi amacıyla otomatik olarak denetim kayıtlarını tutar. Denetim kayıtlarının içeriği ve tutulma yöntemi TOE tarafından sunulan arayüz üzerinden ayarlanabilmektedir. Denetim kayıtlarında yer alan bilgiler sistem yöneticisi dâhil hiç kimse tarafından değiştirilememekte ve silinememektedir.

TOE, denetim kayıtlarının, denetçiler ve sistem yöneticilerinin anlayabileceği format ve açıklıkta olmasını ve belirli kriterler üzerinden kolay ve hızlı bir şekilde filtrelenmiş raporların hazırlanabilmesini sağlar.

Yönetim: Sistemin yönetiminden sorumlu kullanıcılara, TOE tarafından etkin yönetim mekanizmaları sunulur. Bu mekanizmaların hızlı ve etkin karar almayı kolaylaştırması önem taşımaktadır. TOE'nin yönetimi için sağlanan arayüzler yalnızca özel yetki verilmiş kişilerin erişimine açık olup, diğer arayüzlere göre daha sıkı güvenlik önlemlerine tabi tutulur. Örneğin, bu arayüze erişim ve arayüz bileşenleri üzerinde işlem yapılması, sistem üzerindeki herhangi bir işlem gibi değerlendirilmez. Bu işlemlerin günlük kayıtları "kritik" seviyede değerlendirilerek ayrı işlemlere tabi tutulur.

Veri Koruması: TOE'nin korumakla yükümlü olduğu veriler etkin bir şekilde korunmalıdır. Veri korunmasında verinin kritiklik derecesi de önem taşımaktadır. Verinin kritiklik derecesine göre alınacak önlemler farklılık arz etmelidir. Veriler sadece bulundukları ortamda değil, aynı zamanda aktarım esnasında da korumaya tabi tutulmalıdır.

Hassas Verilerin Şifrelenmesi: Hassas nitelikteki veriler sistem üzerinde şifrelenmiş şekilde tutulur. Şifreleme algoritmaları, geri dönüşümü mümkün olmayacak nitelikte ve mevcut teknolojiyle makul bir sürede kırılamayacak derecede güçlü olmalıdır. Hassas verilere örnek olarak şifreler ve banka kart numaraları verilebilir.

Yedekleme: TOE tarafından korunan verilerin, dokümanların ve denetim kayıtlarının yedeklenmesi TOE tarafından sağlanan rutinlerle gerçekleştirilebileceği gibi harici yedekleme cihazları ile sistemin yedeklerinin alınarak, olası arıza durumlarında ve fiziksel hasarların oluşumunda veri kaybına engel olunması sağlanmaktadır.

1.5. BELGEYE GENEL BAKIŞ

Bölüm 1'de TOE ve Koruma Profilinin tanımı yapılmaktadır. Bu ön bilgi sayesinde güvenlik gereksinimleri ve fonksiyonları daha iyi anlaşılacaktır.

Bölüm 2'de uyumluluk iddiaları açıklanmaktadır. Uyumluluk iddiaları arasında Ortak Kriterler uyumluluk iddiası, Koruma Profili uyumluluk iddiası ve paket uyumluluk iddiası bulunmaktadır. Ayrıca uyumluluk iddiası gerekçelendirilmesi ile bu koruma profiline uyum sağlayacak ST'lerin hangi türden bir uyuma sahip olması gerektiği de ifade edilmektedir.

Bölüm 3'te TOE güvenlik sorunu tanımlanması yapılmakta ve TOE kapsamına giren tehditler, varsayımlar ve kurumsal güvenlik politikaları açıklanmaktadır.

Bölüm 4'te TOE ve TOE çevresine yönelik olarak Bölüm 3'te tanımlanmış olan tehditler, varsayımlar ve kurumsal güvenlik politikalarına karşılık gelen güvenlik hedefleri tanımlanmaktadır.

Bölüm 5, genişletilmiş bileşen tanımları yapılması için ayrılmıştır. Ancak bu koruma profili kapsamında genişletilmiş bileşen tanımı bulunmadığından bu bölüm boş bırakılmıştır.

Bölüm 6'da güvenlik hedeflerini sağlayacak fonksiyonel ve garanti gereksinimlerini de içerecek şekilde güvenlik gereksinimleri Ortak Kriterler Bölüm 2 ve Bölüm 3 altında yer alan bileşenlerden faydalanılarak açıklanmaktadır.

Referanslar kısmında ise kayda değer görülen destekleyici kaynaklara yer verilmektedir.

2. UYUMLULUK İDDİALARI

2.1. ORTAK KRİTERLER UYUMLULUK İDDİASI

Bu koruma profili Ortak Kriterler Sürüm 3.1 Revizyon 4 kullanılarak geliştirilmiştir.

Bu koruma profili Ortak Kriterler Bölüm 2 ile tam uyuma sahiptir.

Bu koruma profili, Ortak Kriterler Bölüm 3 ile tam uyuma sahiptir. EAL2 seviyesi bileşenleri kapsanmakta olup ek olarak ALC_FLR.1 (Temel kusur iyileştirme) ve ALC_LCD.1 (Geliştirici tanımlı yaşam döngüsü modeli) bileşenleri, Ortak Kriterler Bölüm 3 altında tanımlandığı şekilde eklenmiştir. Uyumluluk garanti seviyesi EAL2+'dır.

2.2. KORUMA PROFİLİ UYUMLULUK İDDİASI

Bu Koruma Profili, başka bir Koruma Profiline uyumlu olacak şekilde hazırlanmamıştır.

2.3. PAKET UYUMLULUK İDDİASI

Bu Koruma Profili, Ortak Kriterler Bölüm 3 altında tanımlanan garanti paketlerinden EAL 2 ile uyumlu olup EAL 2 altında listelenen bileşenlere ek olarak ALC_FLR.1 (Temel Kusur İyileştirme) ve ALC_LCD.1 (Geliştirici tanımlı yaşam döngüsü modeli) bileşenlerini Ortak Kriterler Bölüm 3 altında tanımlandığı şekliyle zorunlu kılmaktadır.

2.4. UYUMLULUK İDDİASI GEREKÇESİ

Bu koruma profili herhangi bir başka koruma profiline uyumluluk iddia etmediği için bu bölüm uygulanamaz.

2.5. UYUMLULUK BEYANI

Bu Koruma Profili, "katı uyumluluk" gerektirmektedir.

3. GÜVENLİK SORUNLARININ TANIMI

3.1. GİRİŞ

Bu bölümde, TOE ile ilgili güvenlik tehditlerinin kapsamı ve biçimi açıklanarak bu tehditlere karşı alınması gereken önlemler belirtilecektir. TOE'nin kapsamı dışında olan tehditler varsayımlar bölümünde ele alınmış olup, bu tehditlerin bu koruma profilinden bağımsız olarak önlenebiliyor olduğu varsayılmaktadır. Ayrıca kurumsal güvenlik politikalarına da bu bölüm altında yer verilmektedir.

3.2. TEHDİTLER

3.2.1. TEHDİT KAYNAKLARI (AKTÖRLER)

Saldırgan	TOE'yi kullanma yetkisi bulunmayan, fakat arayüzleri aracılığıyla TOE'ye mantıksal veya fiziksel düzeyde erişimi bulunan kişi veya BT varlığıdır. Saldırgan kötü niyetli, sisteme zarar verme yönünde kuvvetli motivasyona ve gerekli bilgi birikimine, sistem kaynağına ve zamana sahiptir.
Sistem_Yöneticisi	TOE'yi yönetme yetkisine sahip kullanıcıdır. Sistem_Yöneticisi TOE'nin işlevsel özellikleri ve yönetimi konularında derin bilgi birikimine sahip olup gerekli eğitimleri almıştır. Ancak hata yapma olasılığı bulunmaktadır. Sistem_Yöneticisi'nin görevini icra etme esnasında herhangi bir art niyeti bulunmaz, bu aktör için geçerli olan tehditler kasıt olmaksızın söz konusu olabilmektedir.
Kullanıcı	TOE'ye yönetim seviyesinde erişim yetkisi bulunmayan, ağ arayüzleri aracılığıyla TOE ile veri alışverişinde bulunan, TOE'yi kapalı bir kutu gibi kullanan son kullanıcıdır. Bu aktörün TOE'ye erişimi esnasında herhangi bir art niyeti bulunmaz, bu aktör için geçerli olan tehditler kasıt olmaksızın söz konusu olabilmektedir.

3.2.2. TEHDİTLER

T.YANILTMA	Saldırgan, TOE'ye sahte bir kimlik kullanarak erişim sağlamak için teşebbüste bulunabilir. Bu teşebbüs, çalınmış bir kullanıcı kimlik bilgisi veya sahte bir IP adresi kullanılarak yapılabilir. Varsayılan kullanıcı adları ve şifrelerin değiştirilmemesi, basit şifrelerin kullanımı, test hesaplarının aktif sistemde de bulunması gibi güvenlik açıklarından faydalanan Saldırgan, TOE'ye yetkisiz erişim sağlayabilir. Bu tehdidin yaygın olarak kullanılan bir örneğinde Kullanıcı veya Sistem_Yöneticisi, Saldırgan tarafından uygulamanın bulunduğu adresten farklı bir adrese yönlendirilerek ve bu adresin TOE'ye ait olduğu izlenimi edinmeleri sağlanarak, sisteme erişim için kullandıkları bilgiler ele geçirilebilir.
T.VERİ_DEĞİŞMESİ	TOE tarafından korunan bir veri, yetkisiz kişilerce izinsiz olarak değiştirilebilir. Örneğin Saldırgan tarafından TOE ile TOE'nin çalışma ortamı bileşenleri

	arasındaki ağ üzerinde taşınan bilgiyi izinsiz olarak değiştirebilir. Veri aktarımı esnasında veri bütünlüğünün temin edildiği protokollerin tercih edilmemesi, bu tehdidin ortaya çıkmasını kolaylaştırmaktadır. Bu tehdidin diğer bir yansıması ise TOE'nin kaynak kodlarının Saldırgan tarafından değiştirilmesidir. Dosya izinlerinin yetersiz olduğu veya TOE'ye yüklenen dosyaların kontrolünün dikkatli yapılmadığı durumlarda bu tehdit söz konusu olabilmektedir.
T.İNKÂR_ETME	TOE üzerinde gerçekleştirilen bir işlemin veya işlemler bütününün (transaction) yapıldığını inkâr edilebilir. Özellikle kurallara uygun ve yeterli düzeyde denetim bileşenleri barındırmayan sistemlerde yapılan bir işlemin veya işlemler bütününün inkâr edilebilmesi kolaylaşmaktadır.
T.VERİ_İFŞASI	TOE tarafından korunan özel bir verinin izinsiz olarak ifşa edilmesidir. Örneğin bir kişinin yetkisi olmadığı halde bir tablo ya da dosyanın içeriğine ulaşması veya ağ üzerindeki açık metinlerin izlenmesi bu kapsamda değerlendirilebilir. Özellikle hassas nitelikteki verilerin şifrelenmeden taşınması bu tehdidi kolaylaştıran bir hususdur.
T.HİZMET_ENGELLEME	Bir hizmetin veya sistemin bir süreliğine kullanılamaz veya erişilemez hale getirilmesidir. Örneğin Saldırgan, TOE'ye sürekli ve yoğun talepte bulunarak TOE'nin bunlara cevap veremez hale gelmesini sağlayabilir. Hizmet engellemenin bir ileri seviyesi olan dağıtık hizmet engelleme saldırıları, ayrıca değerlendirilmesi gereken tehditlerdir. Ancak bu tehditlerin engellenmesi için genellikle yazılım katmanında alınan önlemler yeterli olmaz. Önemli bir husus olmakla birlikte, dağıtık hizmet engelleme saldırıları bu koruma profilinin kapsamına dahil edilmemiştir.
T.YETKİ_YÜKSELMESİ	Yetki yükselmesi, sınırlı yetkilere sahip bir kullanıcının daha yetkili bir kullanıcının yetkilerini alması durumudur. Tehdit kaynaklarından Kullanıcı'nın iyi niyetli olduğu varsayılmaktadır. Ancak Saldırgan, T.YANILTMA tehdidiyle ilgili yöntemleri kullanarak sisteme erişim sağlayıp, daha sonra yetki yükselmesi ile daha üst seviye bir yetkiye sahip olabilir.
T.ZARARLI_VERİ_GİRİŞİ	Saldırgan, zararlı içeriğe sahip bir bilgiyi TOE dışından TOE içine yükleyebilir/taşıyabilir.
T.GÜNLÜK_KÖTÜ_KULLANIM	Saldırgan, güvenlikle alakalı olarak günlük kayıtlarının tutulması fonksiyonunu devre dışı bırakabilir (örneğin depolama alanının yetersiz bırakılması suretiyle). Saldırgan, günlüklere hatalı kayıtlar ekleyerek günlük kayıtlarına duyulan güveni azaltabilir veya Sistem_Yöneticisi'ni sorunların çözümü esnasında yanlış yönlendirebilir.
T.ARTIK_VERİ	Saldırgan, TOE'nin önceki kullanıcı işlemleri sonrasında veya kullanıcı işlemleri sırasında oluşan artık verilere ya da TOE'nin kendi iç işlemleri veya çevresi ile iletişimi sonrası oluşan artık verilere ulaşabilir. Bu veriler kullanıcılara ya da sisteme ait kritik veriler olabilir.

3.3. KURUMSAL GÜVENLİK POLİTİKALARI

P. DENETİM	TOE ve çalışma ortamı bileşenleri için, güvenlikle ilgili tüm olaylar, ilgili faaliyetlerin sorumluluklarını izlemek için kaydedilmeli, korunmalı ve belirli periyotlarla gözden geçirilmelidir.
P.EĞİTİM	Kullanıcıya sistemi kullanmaya başlamadan önce (örneğin giriş ekranında) kolaylıkla fark edilebilecek şekilde kullanım şart ve kısıtlarını, yasal yükümlülükleri ve kullanıcının sistemi kullanmakla kabul etmiş sayılacağı hususlar ve benzeri bilgiler kullanıcıya kolay anlaşılır ifadelerle sunulmalıdır. Kullanıcının kendisine yapılan bildirileri okuyup kabul ettiğinden emin olunmalıdır.

3.4. VARSAYIMLAR

Web uygulamalarına yönelik olan bu koruma profili hazırlanırken yapılmış olan varsayımlar personel ile ilgili varsayımlar, fiziksel ortamla ilgili varsayımlar ve bağlantı ile ilgili varsayımlar olmak üzere üç ana başlıkta toplanmıştır.

Personel ile ilgili varsayımlar:

A.KULLANICI	TOE ve TOE'nin bulunduğu ortam üzerindeki BT varlıklarının kurulum, konfigürasyon ve işletim görevlerinden sorumlu tüm kullanıcıların yeterli derecede tecrübeli, eğitimli ve gerekli güvenlik gereksinimlerini sağladıkları varsayılmaktadır.
A.YÖNETİM	TOE'nin kurulum, konfigürasyon ve işletiminin yetkili kullanıcılar tarafından TOE Kullanım talimatları dokümanlarında belirtildiği üzere doğru olarak yapıldığı varsayılmaktadır.

Fiziksel ortamla ilgili varsayımlar:

A.FİZİKSEL	TOE'nin etkileşim içinde olduğu çalışma ortamı bileşenleri ile ilgili gerekli fiziksel ve çevresel güvenliğin sağlanmış olduğu varsayılmaktadır. Sunucunun bulunduğu odaya girişler önceden belirlenmiş yetkilendirme kurallarına göre yapılması ve bunların kayıtlarının tutulması gerekmektedir.
A.BT_VARLIKLARI	TOE'nin etkileşim içinde olduğu çalışma ortamındaki tüm BT varlıklarının gerekli güvenlik gereksinimlerinin sağlanmış olduğu varsayılmaktadır. Bunlardan yazılım bileşenleri sahip olanların en son güvenlik güncellemelerinin yapılmış olduğu ve güvenlik için önerilen konfigürasyon ayarlarının yapılmış olduğu varsayılmaktadır.

A.YEDEKLEME	TOE tarafından üretilen ve TOE'ye dışarıdan dahil edilen her türlü verinin, bu verinin tutulduğu depolama birimi ve donanım yedeğinin, sistemin çökmesi durumunda hiç bir veri kaybı olmayacak şekilde yedeklendiği varsayılmaktadır.

Bağlantı ile ilgili varsayımlar

A.İLETİŞİM	TOE'nin etkileşim içinde olduğu uzak (remote) bir BT sistemi üzerinden yapılan veya uzak bir BT sistemine yapılan tüm iletişim ve iletişimin yapıldığı ağın güvenliğinin sağlanmış olduğu varsayılmaktadır.

4. GÜVENLİK HEDEFLERİ

4.1. GİRİŞ

Bu bölümde TOE güvenlik hedefleri ile TOE'nin Çalışma ortamı için güvenlik hedefleri açıklanmaktadır.

Güvenlik hedefleri, TOE için Güvenlik Hedefleri (TOE tarafından direkt olarak adreslenen güvenlik hedefleri) ve TOE Çalışma ortamı için güvenlik hedefleri (BT ortamı tarafından adreslenen veya teknik olmayan güvenlik hedefleri) olarak iki bölümde incelenmiştir. Bu güvenlik hedefleri güvenlik ihtiyaçlarının karşılanmasında TOE ve çevresinin sorumluluklarını belirlemektedir.

4.2. DEĞERLENDİRME HEDEFİ İÇİN GÜVENLİK HEDEFLERİ

O. DENETİM	TOE, veri erişimleri, sistem fonksiyonlarına erişim ve güvenlik ile ilgili yapılan işlemlerin tamamını kayıt altına almalı, kayıtları korumalı ve kayıtların değiştirilmediğinden emin olmalıdır. Bu kayıtlar sürekli olarak kolay ve hızlı bir şekilde izlenebilmeli, gerektiğinde kritik kayıtların yönetici düzeyindeki kullanıcılara bildirilmesi konusunda ek önlemler alınmalıdır.
O. YETKİLENDİRME	TOE, sistemde tanımlı olan tüm kullanıcıların her birinin birbirinden farklı olarak tanımlanmasını sağlamalı, bu kullanıcıları farklı seviyelerle yetkilendirebilmeli ve sisteme erişim izni vermeden önce kullanıcının kimliğini doğrulamalıdır. Belirli bir kullanıcı veya kullanıcı grubuna özel yetkiler (örneğin belirli tipteki belgelere erişim yetkisi gibi) verilebilmelidir. DH'ye yapılan tüm isteklerde yetki kontrolü süreci uygulanarak veri veya belgelere yalnızca yetki sahibi kullanıcıların eriştiğinden emin olunmalıdır.
O. BİLGİ_AKIŞI_KNTRL	TOE içeriden dışarıya veya dışarıdan içeriye izinsiz bilgi çıkış ve girişlerini kontrol etmeli ve yönetmelidir. TOE tarafından alınan her bilgi bir denetim mekanizmasından geçilerek içerik kontrolüne tabi tutulmalıdır.
O. YÖNETİM	TOE, TEO üzerinde yönetici yetkisine sahip kullanıcıların sistemi güvenli ve etkin bir şekilde yönetebilmeleri için gerekli tüm araç ve fonksiyonları sağlamalıdır. Bu araç ve fonksiyonları yetkisiz erişim ve kullanımlara karşı kısıtlamalı ve gerekli

	güvenlik önlemlerini almalıdır. Kullanıma sunulan araçların hızlı, etkin ve kolay karar alma imkanı sunduğundan emin olunmalıdır.
O. BİLGİNİN_KORUMASI	TOE, sistem üzerindeki verilerinin yetkisiz olarak görüntülenmesi, değiştirilmesi ve silinmesine karşı gerekli güvenlik önlemlerini sağlamalıdır.
O. HATA_YÖNETİMİ	TOE, sistem üzerindeki verilerinin yetkisiz olarak görüntülenmesi, değiştirilmesi ve silinmesine karşı gerekli güvenlik önlemlerini sağlamalıdır.
O.ARTIK_VERİ	TOE, koruma altındaki bir kaynak üzerindeki kritik verilere artık ihtiyaç duyulmadığında erişilmez olmasını sağlamalıdır.
O.FONKSİYONEL_TEST	TOE'nin, tüm güvenlik fonksiyonel gereksinimlerini sağlamasını temin etmek amacıyla, TOE'ye güvenlik fonksiyonel testleri uygulanmalıdır.

4.3. ÇALIŞMA ORTAMI İÇİN GÜVENLİK HEDEFLERİ

OE.FIZIKSEL GÜVENLIK	TOE çalışma ortamı güvenlik hedefleri, etki alanı içindeki BT varlıklarının fiziksel olarak güvenliğini sağlamalıdır. Yetkisiz olmayan kişilerin bu ortama giriş çıkışlarının engellenmesi gerekmektedir.
OE.GÜVENİLİR_KULLANICI	TOE çalışma ortamı güvenlik hedefleri, TOE çalışma ortamı üzerinde yetkili tüm kullanıcıların gerekli eğitimleri almış ve tüm güvenlik gereksinimlerini sağlamış olmalarını sağlamalıdır.
OE.DENETİM_VE_İZLEME	TOE'nin bulunduğu çalışma ortamına yapılan tüm giriş-çıkışların kontrol altında tutulması ve kayıt altına alınması gerekmektedir. Bu kayıtlar sürekli olarak izlenmeli ve gerektiğinde bu kayıtlar üzerinde inceleme yapılabilmesine imkân sağlanmalıdır.
OE.ZAMAN_DAMGALARI	TOE çalışma ortamı güvenlik hedefleri, güvenlikle ilgili olay kayıtlarının zamanlarının yeterince hassas olarak kaydedilmesi için zaman damgalarının oluşturmasını sağlamalıdır.
OE.İLETİŞİM	TOE çalışma ortamı TOE için güvenilir bir iletişim ortamı sağlamalıdır.
OE.YÖNETİM	TOE nin teslimatı, kurulumu, yönetimi ve operasyonel işleri yapılırken BT güvenlik gereksinimlerine tutarlı bir şekilde bu işlemler yapılmalıdır.
OE.TEST ORTAMI	TOE üzerinde testler sırasında kullanılmak için hazırlanmış fonksiyon ve parametler kaldırılmalı veya kullanılamaz hale getirilmelidir.

OE. BT_VARLIKLARI	TOE'nin çalışma ortamında bulunan TOE etkileşim içinde olduğu tüm BT varlıklarının güvenliği sağlanmalıdır. Bu varlıklara sadece özel olarak yetkilendirilmiş kullanıcılar giriş yapabilmelidir.
OE.YEDEKLEME	TOE'nin çalışma ortamında tutulan tüm verilerin, problem oluşması durumunda veri kaybı oluşmayacak şekilde tanımlanmış rutinlerle yedeklenmesi sağlanmalıdır.

4.4. GÜVENLİK HEDEFLERİ GEREKÇESİ

Güvenlik hedeflerinin gerekçesi; belirtilen güvenlik hedeflerinin, güvenlik ile ilgili sorunları takip etmek için gerekli, uygun ve yeterli olduğunu göstermektedir.

Güvenlik hedeflerinin gerekçesinde şu hususlar doğrulanmıştır:

- Her bir tehdit, kurumsal güvenlik politikası ve varsayımın takibi için en az bir güvenlik hedefi tanımlanmıştır.
- Her bir güvenlik hedefi en az bir tehdit, kurumsal güvenlik politikası ve varsayıma karşılık gelmektedir.

4.4.1. GÜVENLİK HEDEFLERİNİN KAPSAMI

Tablo 1, Güvenlik Problem Tanımlarının, hangi güvenlik hedefi tarafından kapsandığını göstermektedir. Tehditler ve Kurumsal güvenlik hedefleri TOE için güvenlik hedefleri ve çalışma ortamı için güvenlik hedefleri ile ele alınmaktadır. Varsayımlar ise sadece TOE çalışma ortamı için güvenlik hedefleri ile ele alınmaktadır.

Tablo 1: Güvenlik Sorunları ile Güvenlik Hedefleri Arasındaki İlişkiler

		Tehditler									KGP		Varsayımlar				
		T.YANILTMA	T.VERİ_DEĞİŞMESİ	T.İNKÂR_ETME	T.VERİ_İFŞASI	T.HİZMET_ENGELLEME	T.YETKİ_YÜKSELMESİ	T.ZARARLI_VERİ_GİRİŞİ	T.GÜNLÜK_KÖTÜ_KULLANIM	T.ARTIK_VERİ	P.DENETİM	P.EĞİTİM	A.KULLANICI	A.YÖNETİM	A.FİZİKSEL	A.BT_VARLIKLARI	A.İLETİŞİM
Güvenlik Hedefleri	O.DENETİM	X		X		X	X		X		X						
	O.YETKİLENDİRME	X	X			X	X										
	O.BİLGİ_AKIŞI_KNTRL		X	X				X									
	O.YÖNETİM		X														
	O.BİLGİNİN_KORUMASI		X		X		X										
	O.HATA_YÖNETİMİ				X		X										
	O.ARTIK_VERİ	X								X							
	O.FONKSİYONEL_TEST	X	X	X	X	X	X	X	X	X							
Çalışma Ortamı Güv. Hed.	OE.FIZIKSEL GÜVENLIK														X		
	OE.GÜVENİLİR_KULLANICI											X	X				
	OE.DENETİM										X				X	X	
	OE.ZAMAN DAMGALARI										X						
	OE.İLETİŞİM																X
	OE.YÖNETİM													X			
	OE.TEST ORTAMI													X			
	OE.BT_VARLIKLARI															X	

4.4.2. TOE İÇİN GÜVENLİK HEDEFLERİNİN GEREKÇESİ

O. DENETİM

TOE, sistem fonksiyonlarına erişim ve güvenlik ile ilgili yapılan işlemlerin tamamının kayıt altına alınmasını sağlar. Bu kayıtları güvenli bir şekilde korunmasına ve gerektiğinde bu kayıtların izlenmesine olanak verir. TOE tarafından, denetim datası dolması durumunda aksiyon alınması için bir fonksiyon sağlar. Denetim datasının üretilmesi, ardışık kimlik doğrulama girişimleri sırasında TOE'nin denetim datasını kullanarak saldırganın kimliğini tespit edebilmesini sağlar. Denetim kayıtları, sahte kimlik kullanım ile yanıltma, belirli bir işlem yada işlemler bütünün inkar edilmesi,

hizmetin veya sistemin engellenmesi, izinsiz yetki yükseltmesi ve günlüklerin kötü kullanımı gibi güvenlik sorunlarını engeller.

Bu nedenle, T.YANILTMA, T.İNKÂR_ETME, T.HİZMET_ENGELLEME, T.YETKİ_YÜKSELMESİ, T.GÜNLÜK_KÖTÜ_KULLANIM tehditlerine karşı önlem sağlar ve P. DENETİM kurumsal güvenlik politikasının yapılmasını garanti altına alır.

O. YETKİLENDİRME

Bu güvenlik hedefi kullanıcıların yetkilendirilmesini ve kimlik doğrulamasının yapılmasını sağlar. Her iki işlemde güvenlik ile ilgili işlemlerin yönetilmesi için gereklidir. TOE, Sisteme erişmek isteyen tüm kullanıcıların kimlik doğrulamasını yaptıktan sonra kullanıcıların sisteme kendi yetkileri dâhilinde erişimlerini sağlar. Sistem yöneticilerinin tanımlanması sistem üzerinde gerçekleşen eylemlerinin sorumluluklarının sistem yöneticisi tarafından alınması için gereklidir.

TOE erişim için gerekli kimlik doğrulama, ancak harici bir saldırgan tarafından yapılan üst üste kimlik doğrulama girişimlerine karşı savunmasız olabilir. Bu nedenle TOE harici bir saldırgan tarafından yapılan üst üste kimlik doğrulama girişimlerine karşı bir savunma mekanizması sağlayacaktır.

Bu nedenle, T.YANILTMA, T.VERİ_DEĞİŞMESİ, T.HİZMET_ENGELLE-ME, T.YETKİ_YÜKSELMESİ, tehditlerine karşı önlem sağlar.

O. BİLGİ_AKIŞI_KNTRL

Bu güvenlik hedefi, TOE içeriden dışarıya veya dışarıdan içeriye izinsiz bilgi çıkış ve girişlerini kontrol edilmesini sağlar. Böylece bilgi akışı üzerinden gelebilecek saldırılar belirlenir ve önlenir. Bu saldırılar zararlı bilgi kullanılarak yapılan bir saldırı veya web uygulamasına yetkisiz bir erişim olabilir.

Bu nedenle, T.VERİ_DEĞİŞMESİ, T.İNKÂR_ETME, T.ZARARLI_VE-Rİ_GİRİŞİ tehditlerine karşı önlem sağlar.

O. YÖNETİM

Bu güvenlik hedefi, sistem_yöneticisi yetkisine sahip kullanıcıların sistemi güvenli ve etkin bir şekilde yönetebilmeleri için gerekli tüm araç ve fonksiyonları sağlar. Bu güvenlik hedefi sayesinde TOE'nin güvenlik fonksiyonu verilerinin güncel tutulmasına da olanak verir.

Bu nedenle, T.VERİ_DEĞİŞMESİ tehditlerini karşı önlem sağlar.

O. BİLGİNİN_KORUNMASI

Bu güvenlik hedefi, sistem üzerindeki TOE'nin güvenlik fonksiyonu verilerinin yetkisiz olarak görüntülenmesi, değiştirilmesi ve silinmesine karşı gerekli güvenlik önlemlerini sağlar.

Bu nedenle, T.VERİ_DEĞİŞMESİ, T.VERİ_İFŞASI, T.YETKİ_YÜKSELMESİ tehditlerine karşı önlem sağlar.

O. HATA_YÖNETİMİ

Bu güvenlik hedefi, tüm hata durumları yönetilmesini ve kullanıcılara hataların TOE'nin güvenlik fonksiyonu verilerini içermeden daha anlamlı hale getirerek sunulmasını sağlar. Böylece sistemin hata vermesi üzerine yapılan saldırılarda

sistem hata yönetimi yaparak veri ifşası ve yetkisiz erişim gibi güvenlik sorunlarının engellenmesini sağlar.

Bu nedenle, T.VERİ_İFŞASI, T.YETKİ_YÜKSELMESİ tehditlerine karşı önlem sağlar.

O.ARTIK_VERİ

Bu güvenlik hedefi, TOE tarafından yürütülen işlemler sırasında veya sonrasında, bu işlemler tarafından kullanılan verilere yetkisiz bir şekilde erişilememesini sağlar.

Bu nedenle, T.YANILTMA ve T.ARTIK_VERİ tehditlerine karşı önlem sağlamaktadır.

O.FONKSİYONEL_TEST

Bu güvenlik hedefi TOE'nin tüm güvenlik fonksiyonel gereksinimlerini sağlamasını temin etme amacını taşımaktadır.

Bu nedenle bu hedef diğer hedeflerin etkinliğini artırması beklenen genel bir hedef niteliğinde olup, TÜM TEHDİTLERE KARŞI önlem sağlamaktadır.

4.4.3. ÇALIŞMA ORTAMI İÇİN GÜVENLİK HEDEFLERİNİN GEREKÇESİ

OE. FİZİKSEL_GÜVENLİK

Bu çalışma ortamı güvenlik hedefi, TOE'nin fiziksel olarak güvenli bir ortamda bulunmasını ve işletiminin yapılmasını sağlar. Yetkisiz olmayan kişilerin bu ortama giriş çıkışlarını engeller.

Bu nedenle, A.FİZİKSEL varsayımına karşı önlem sağlar.

OE. GÜVENİLİR_KULLANICI

Bu çalışma ortamı güvenlik hedefi, TOE çalışma ortamı üzerinde yetkili tüm kullanıcıların gerekli güvenlik denetimlerinden geçmelerini ve güvenlik eğitimin almış tecrübeli kişilerden seçilmelerini sağlar.

Bu nedenle, P.EĞİTİM kurumsal güvenlik politikasına ve A.KULLANICI varsayımına karşı önlem sağlar.

OE. DENETİM_VE_İZLEME

Bu çalışma ortamı güvenlik hedefi, TOE nin bulunduğu çalışma ortamına yapılan tüm giriş çıkışların kayıt altına alınmasını sağlar. Bu kayıtları güvenli bir şekilde korunmasına ve gerektiğinde bu kayıtların izlenmesine olanak verir. Ortama yetkisiz erişimlerin yapılması engeller.

Bu çalışma ortamı güvenlik hedefi aynı zamanda TOE nin bulunduğu çalışma ortamındaki IT varlıklarına yapılan güvenlikle ilgili erişimlerinde kayıt altına alınmasını sağlar. Bu kayıtları güvenli bir şekilde korunmasına ve gerektiğinde bu kayıtların izlenmesine olanak verir.

Bu nedenle, A.FİZİKSEL ve A.BT_VARLIKLARI varsayımlarına karşı önlem sağlar ve P.DENETİM kurumsal güvenlik politikasının yapılmasını garanti altına alır.

OE. ZAMAN DAMGALARI	Bu çalışma ortamı güvenlik hedefi, güvenlikle ilgili olay kayıtlarını zamanlarının yeterince hassas olarak kaydedilmesi için zaman damgalarının oluşturmasını sağlar. Bu nedenle, P.DENETİM kurumsal güvenlik politikasının tam olarak doğru çalışıyor olmasını garanti altına alır.
OE. İLETİŞİM	Bu çalışma ortamı güvenlik hedefi, TOE çalışma ortamındaki network'ün güvenilir bir iletişim ortamı sağlamasına olanak verir. Bu nedenle, A.İLETİŞİM varsayımına karşı önlem sağlar.
OE. YÖNETİM	Bu çalışma ortamı güvenlik hedefi, TOE'nin kurulumu, yönetimi ve işletimi ile ilgili görevlerin TOE'nin kurulum talimatları dokümanlarına uygun olarak ve BT güvenlik gereksinimlerine tutarlı bir şekilde yapılmasını sağlar. Bu nedenle, A.YÖNETİM varsayımına karşı önlem sağlar.
OE. TEST ORTAMI	Bu çalışma ortamı güvenlik hedefi, TOE üzerinde testler sırasında kullanılmak için hazırlanmış fonksiyon ve parametreler kaldırılmasını veya kullanılamaz hale getirilmesini sağlar. Bu nedenle, A.YÖNETİM varsayımına karşı önlem sağlar.
OE. BT_VARLIKLARI	Bu çalışma ortamı güvenlik hedefi, TOE'nin çalışma ortamında bulunan tüm BT varlıklarının BT güvenlik gereksinimlerine göre güvenliğinin alınmasını sağlar. Bu nedenle, A.BT_ VARLIKLARI varsayımına karşı önlem sağlar.

5. GENİŞLETİLMİŞ BİLEŞENLER TANIMI

Bu koruma profili, genişletilmiş bir bileşene ihtiyaç duymamaktadır.

6. GÜVENLİK GEREKSİNİMLERİ

6.1. FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ

6.1.1. GENEL BAKIŞ

Bu koruma profilinde kapsanan bileşenler, aşağıda tablo halinde sunulmaktadır.

Tablo 2: Kapsanan Fonksiyonel Güvenlik Gereksinimlerinin Listesi

Kod	Uzun İsim
FAU_GEN.1	Denetim verilerinin oluşturulması
FAU_GEN.2	Kullanıcı kimliğinin ilişkilendirilmesi
FAU_SAR.1	Denetimin gözden geçirilmesi
FAU_SAR.2	Kısıtlanmış denetimin gözden geçirilmesi
FAU_SAR.3	Seçmeli denetimin gözden geçirilmesi
FAU_STG.1	Korunmuş denetim takibi belleği
FAU_STG.3	Denetim kayıtlarının olası kaybı halinde eylem
FAU_STG.4	Denetim verileri kaybının önlenmesi
FDP_ACC.1	Alt küme erişim kontrolü
FDP_ACF.1	Güvenlik özniteliğine dayalı erişim kontrolü
FIA_UID.1	Tanınmanın zamanlaması
FMT_MOF.1	Güvenlik fonksiyonları davranışının yönetimi
FMT_MSA.1	Güvenlik özelliklerinin yönetimi
FMT_MTD.1	TSF verilerinin yönetimi
FMT_SMF.1	Yönetim fonksiyonlarının belirlenmesi
FMT_SMR.1	Güvenlik rolleri
FPT_FLS.1	Başarısızlık durumunda güvenli durumun korunması
FPT_STM.1	Güvenilir zaman etiketleri
FRU_FLT.1	İndirgenmiş hata toleransı
FTA_MCS.1	Eşzamanlı çoklu oturumlar üzerindeki temel sınırlama
FTA_SSL.3	TSF tarafından başlatılmış sonlandırma
FTA_SSL.4	Kullanıcı tarafından başlatılmış sonlandırma
FTA_TAH.1	TOE erişim tarihi
FTA_TSE.1	TOE oturumu kurma
FTP_ITC.1	TSF arası güvenilir kanal
FTP_TRP.1	Güvenilir yol

6.1.2. FONKSİYONEL GÜVENLİK POLİTİKALARI

Erişim Kontrol Politikası

Erişim Kontrol Politikası, web uygulaması tarafından saklanan verilere erişimle ilgili hususları düzenleyen politikadır. Bu politikaya ilişkin detaylar, FAU_ACC.1 ve FAU_ACF.1 bileşenleri altında açıklanmaktadır.

6.1.3. GÜVENLİK DENETİMİ (FAU)

FAU_GEN.1 Denetim verilerinin oluşturulması

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FPT_STM.1 Güvenilir zaman mühürleri

FAU_GEN.1.1: TSF'nin aşağıdaki denetlenebilir olayların bir denetim kaydını oluşturabilmesi gerekir:

a) Denetim fonksiyonlarının başlatılması ve kapatılması,

b) Denetimin **[temel]** düzeyi için tüm denetlenebilir olaylar,

c) Tüm yetkilendirme (authentication) girişimleri (başarılı ve başarısız),

d) Sistem_Yöneticisi seviyesindeki kullanıcıların yetki ve rol değişiklikleri ve

c) **[Diğer denetlenebilir olaylar için Tablo 3'e bakınız]**.

FAU_GEN.1.2: TSF'nin her bir denetim kaydı içerisinde en azından aşağıdaki bilgileri kaydetmesi gerekir:

a) Olayın tarihi ve zamanı, olay tipi, özne kimliği (uygun ise) ve olayın sonucu (başarı ya da başarısızlık) ve

b) Her bir olay denetimi tipi için, PP/ST içerisinde yer alan fonksiyonel öğelerin denetlenebilir olay tanımlamalarına dayanarak, [atama: şu bilgiler kayıt edilmelidir: öznenin oturum (session) bilgisi, özne tarafından gönderilen işlem parametreleri].

Uygulama Notu: Sistem_Yöneticisi'nin denetime konu olacak eylemleri seçebilme imkânı olmalıdır. Bu durum denetime konu olacak eylemlerin listesinin dinamik olmasını gerektireceğinden, seçilen eylemlerin değişiminin de denetime tabi olması gerekir. TOE aracılığıyla gerçekleşen eylemlerin sonucu, tek haneli başarı veya başarısızlık durumu ile ifade edilebileceği gibi, TOE'nin sistem tasarımına göre değişecek şekilde daha geniş bir sonuç kümesine de sahip olabilir. Bununla birlikte, başarılı ve başarısız eylemler hızlı ve kolay bir şekilde gözlemlenebilmeli, ayrıca otomatik yöntemlerle ayırt edilebilir olmalıdır. Tüm yetkilendirme girişimlerinin denetim altına alınması gerektiği ifade edilmiştir, ancak Sistem_Yöneticisi'nin bu denetimleri belirli kullanıcılar veya kullanıcı grupları için, belirli yetkilendirme yöntemleri için filtrelemesi ve böylelikle denetim kayıtlarının fazla alan kaplaması isteniyorsa bu bileşene ek olarak FAU_SEL.1 bileşeninin de seçilmesi düşünülebilir.

Uygulama Notu: Olay tarihi ve zamanı olarak web uygulamasının üzerinde çalıştığı sunucudan temin edilen tarih ve zaman bilgisi kullanılır. Sunucudan edinilen bilginin hata payına sahip olma ihtimali bulunmakla birlikte bu hata payı göz ardı edilebilecek seviyede olduğu sürece bu durum güvenlik açısından bir sorun oluşturmayacaktır. TOE'nin farklı bileşenleri arasındaki zaman koordinasyonundan ve bu zamanların genel itibariyle doğruya oldukça yakın olmasından Sistem_Yöneticisi sorumludur.

Rasyonel: Bu bileşen, denetim kayıtlarının tutulması ile ilgili detayları barındırması sebebiyle O.DENETİM hedefine katkı sağlar.

Tablo 3: Denetime Tabi Tutulacak Olaylar

Bileşen	Olay	Detay Bilgi
FAU_SAR.1	Denetim kayıtlarından veri okunması	
FAU_SAR.2	Denetim kayıtlarından veri okumanın amaçlandığı başarısız girişimler	
FAU_SEL.1	Denetime konu olan olayları düzenlemeye çalışan kullanıcının kimlik bilgisi	
FAU_STG.3	Eşik değerin aşılması halinde uygulanacak eylemler	
FAU_STG.4	Denetime ayrılmış depolama biriminin hatası halinde yapılacak eylemler	
FDP_ACF.1	Fonksiyonel güvenlik politikası tarafından kapsanan bir nesne üzerindeki tüm işlem girişimleri	Nesneye ait tanımlama bilgisi
FIA_UID.1	Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı	Sunulan kullanıcı kimliği,

Bileşen	Olay	Detay Bilgi
	kimliğini de içeren, başarısız kullanımı, Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı kimliğini de içeren, bütün kullanımı.	girişimin kaynağı (bağlanan uç tanımlayıcısı, kaynak adres gibi)
FMT_MOF.1	TSF içerisindeki fonksiyonların davranışındaki tüm değişiklikler.	
FMT_MSA.1	Güvenlik özelliklerinin değerlerinin tüm değişiklikleri.	
FMT_MTD.1	TSF verilerinin değerlerine yönelik tüm değişiklikler.	
FMT_SMF.1	Yönetim fonksiyonlarının kullanımı.	
FMT_SMR.1	Bir rolün parçası olan kullanıcıların grubuna yönelik değişiklikler.	
FPT_FLS.1	TSF hatası.	
FPT_STM.1	Tarih/saatin belirli bir değere atanması	Tarih/saat için eski ve yeni değerler
FRU_FLT.1	TSF tarafından bulunmuş olan herhangi bir hata. Bir hata nedeniyle kesintiye uğramış olan tüm TOE özellikleri.	
FTA_MCS.1	Eşzamanlı çoklu oturumun sınırlanmasına dayanarak yeni bir oturumun reddedilmesi.	
FTA_SSL.3	Oturum kilitleme mekanizması tarafından etkileşimli bir oturumun bitirilmesi.	
FTA_SSL.4	Kullanıcı tarafından etkileşimli bir oturumun bitirilmesi.	
FTA_TSE.1	Oturum kurma mekanizmasından dolayı bir oturum kurulmasının reddedilmesi. Bir kullanıcı oturumu kurulması için tüm denemeler.	
FTP_ITC.1	Güvenilir kanal fonksiyonlarının başarısızlığı. Başarısız güvenilir kanal fonksiyonlarının başlatıcısının ve hedefinin kimliğinin belirlenmesi. Güvenilir kanal fonksiyonlarının kullanılması için bütün denemeler. Bütün güvenilir kanal fonksiyonlarının başlatıcı ve hedeflerinin kimliğinin belirlenmesi.	
FTP_TRP.1	Güvenilir yol fonksiyonlarının başarısızlıkları. Eğer varsa, bütün güvenilir yol başarısızlıklarıyla ilgili kullanıcının kimliğinin belirlenmesi. Güvenilir yol fonksiyonlarının kullanılması için bütün denemeler. Eğer varsa, bütün güvenilir yol talepleriyle bağlantılı kullanıcının kimliğinin belirlenmesi.	

FAU_GEN.2 Kullanıcı kimliğinin ilişkilendirilmesi

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FAU_GEN.1 Denetim verilerinin oluşturulması

FIA_UID.1 Tanıma zamanı

FAU_GEN.2.1: Tanınan kullanıcıların eylemlerinden ortaya çıkan denetleme olayları için TSF'nin her bir denetlenebilir olayı, olaya neden olan kullanıcının kimliğiyle ilişkilendirebilmesi gerekir.

Rasyonel: Bu bileşen, denetim kayıtlarının kullanıcılarla ilişkilendirilmesine imkân tanıması sebebiyle O.DENETİM hedefine katkı sağlar.

FAU_SAR.1 Denetimin gözden geçirilmesi

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FAU_GEN.1 Denetleme verilerinin oluşturulması

FAU_SAR.1.1: TSF'nin [atama: yetkili kullanıcılar]'a denetleme kayıtlarından elde edilen [tüm denetim bilgisi]'ni okuyabilme yeteneğini sağlaması gerekir.

FAU_SAR.1.2: TSF'nin bilginin yorumlanması için denetleme kayıtlarını kullanıcıya uygun olan bir biçimde sağlaması gerekir.

ST Yazarı Notu: Bu bileşenin eklenmesinin amacı, kullanıcının denetim kayıtlarının karmaşıklığından korunarak bu denetim kayıtlarını olay anında etkin ve hızlı bir şekilde karar vermede kullanabilmesini sağlamaktır. Bu bileşenle amaçlanan işlevsellik farklı şekillerde hayata geçirilebilir, ancak bileşenin eklenme amacı göz önünde bulundurularak denetim kayıtlarına etkin ve hızlı erişim sağlanabildiğinden ve kayıtların Sistem_Yöneticisi'ne kolay ve hızlı karar alması konusunda destek olduğundan emin olunmalıdır. Bu bileşenle amaçlanan işlevselliğin harici araçlarla sağlanması, bu bileşenle uyumluluğun temin edildiği anlamına gelir. Bu bileşenle amaçlanan işlevsellik, FAU_SAR.3 bileşeniyle birlikte düşünülerek tasarlanmalıdır. Yetkili kullanıcıların denetim kayıtlarını okumaya yetkili kılınması için seçilen yöntem (örneğin denetim kayıtlarını okuma yetkisine sahip bir rol tanımlanarak ilgili kullanıcılara bu rolün verilmesi, denetim kayıtlarının bir kısmının okunması için ayrı bir rol tanımlanması gibi) belirlenerek ifade edilmelidir.

Rasyonel: Bu bileşen, denetim kayıtlarının kullanıcılar tarafından kolay bir şekilde okunabilmesini sağlaması sebebiyle O.DENETİM ve O.YÖNETİM hedeflerine katkı sağlar.

FAU_SAR.2 Kısıtlanmış denetimin gözden geçirilmesi

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FAU_SAR.1 Denetimin gözden geçirilmesi

FAU_SAR.2.1: TSF'nin açık okuma erişimi hakkı olanlar dışında tüm kullanıcıların denetim kayıtlarına erişimlerini kısıtlaması gerekir.

Uygulama Notu: Bu bileşenle amaçlanan, uygulama seviyesinde bir erişim engellemesidir. İşletim sistemi ve depolama birimi seviyesinde erişim engelleme için gerekli önlemlerin alındığı varsayılmaktadır.

Rasyonel: Bu bileşen, denetim kayıtlarının yalnızca belirlenen kullanıcılar tarafından görülebilmesini sağlaması sebebiyle O.DENETİM ve O.YETKİLENDİRME hedeflerine katkı sağlar.

FAU_SAR.3 Seçmeli denetimin gözden geçirilmesi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: FAU_SAR.1 Denetimin gözden geçirilmesi

FAU_SAR.3.1: TSF'nin [atama: mantıklı ilişkileri olan kriterler]'e dayanarak denetleme verilerinin uygulanması [atama: seçim ve/veya düzenleme yöntemleri] yeteneğini sağlaması gerekir.

ST Yazarı Notu: Bu bileşenin eklenmesinin amacı, kullanıcının denetim kayıtlarının karmaşıklığından korunarak bu denetim kayıtlarını olay anında etkin ve hızlı bir şekilde karar vermede kullanabilmesini sağlamaktır. Bu bileşenle amaçlanan işlevsellik farklı şekillerde hayata geçirilebilir, ancak bileşenin eklenme amacı göz önünde bulundurularak denetim kayıtlarına etkin ve hızlı erişim sağlanabildiğinden ve kayıtların Sistem_Yöneticisi'ne kolay ve hızlı karar alması konusunda destek olduğundan emin olunmalıdır. Bu bileşenle amaçlanan işlevselliğin harici araçlarla sağlanması, bu bileşenle uyumluluğun temin edildiği anlamına gelir.

Rasyonel: Bu bileşen, denetim kayıtlarının kullanıcılara seçime bağlı olarak gösterilmesini sağlamaktadır. Bu nedenle hem O.DENETİM, hem de O.YÖNETİM hedeflerine katkı sağlar.

FAU_STG.1 Korunmuş denetim takibi belleği

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FAU_GEN.1 Denetim verilerinin oluşturulması

FAU_STG.1.1 TSF'nin denetleme takibinde saklanan denetim kayıtlarını yetkisiz silmelerden koruması gerekir.

FAU_STG.1.2 TSF'nin denetleme takibinde saklanan denetim kayıtlarını değiştirmelere karşı **[tespit etme]** yeteneğinde olması gerekir.

Uygulama Notu: Denetim kayıtlarının yetkisiz silmelerden ve değiştirmelerden korunması için alınabilecek en esaslı önlemler işletim sistemi seviyesindeki önlemlerdir. Bu önlemlerin eksiksiz olarak alınmış olduğu varsayılmaktadır. Uygulama seviyesinde ise, silme ve değiştirmenin tespiti mümkündür. FAU_STG.1.1, denetim kayıtlarının yetkisiz silmelerden korunmasını öngörmekle birlikte, TOE'nin çalışma ortamı bileşenlerinden biri veya daha fazlasında bu işlevin yerine getirilmesiyle, bu bileşene uyum sağlanmış olur. Denetim kayıtlarının değiştirilmesinin tespiti ise her durumda TSF tarafından yerine getirilmelidir.

Uygulama Notu: Bazı durumlarda TOE, harici bir bileşen yardımıyla denetim kayıtlarının takibini gerçekleştiriyor olabilir. Bu durumda, harici bileşene ulaşılamaması ihtimalinin ortadan kaldırılması için TOE içerisinde bir tampon belleğin kullanımı faydalı olacaktır. Kullanılan tampon belleğin bu bileşene uyum sağlaması gerekmektedir.

Rasyonel: Bu bileşen, denetim kayıtlarının yetkisiz silme ve değiştirmelerden korunmasını sağlaması sebebiyle O.DENETİM ve O.BİLGİ_KORUNMASI hedeflerine katkı sağlar.

FAU_STG.3 Denetim kayıtlarının olası kaybı halinde eylem

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FAU_STG.1 Korunmuş denetim takibi belleği

FAU_STG.3.1 **Geliştirme:** Eğer denetim kayıtları için **[Sistem_Yöneticisi tarafından belirlenmiş olan sınır]** ~~aşıldıysa~~ **belirlenmiş bir süre sonra aşılacaksa** TSF'nin **[atama: Sistem_Yöneticisi'ni e-posta aracılığıyla bilgilendirme, [seçim: SMS veya eşdeğer bir bilgilendirme yöntemi kullanma, sisteme giriş yapan kullanıcılara durumla ilgili mesaj gösterme]**, olası denetim belleği arızası halinde yapılacak olan eylemler] kararını alması gerekir.

Rasyonel: Bu bileşen, denetim kayıtlarının aralıksız bir şekilde tutulabilmesi için çözümler üretmeyi amaçlar. Bu nedenle O.DENETİM hedefine katkı sağlar. Ayrıca Sistem_Yöneticisi'nin olası bir arıza durumunda olay yönetimine destek sağlaması sebebiyle O.YÖNETİM hedefine de katkı sağlar.

FAU_STG.4 Denetim verileri kaybının önlenmesi

Hiyerarşik Bileşen(ler): FAU_STG.3 Denetim kayıtlarının olası kaybı halinde eylem

Bağımlılıklar: FAU_STG.1 Korunmuş denetim takibi belleği

FAU_STG.4.1 Eğer denetim hafızası doluysa TSF'nin [seçim: 'denetlenebilir olayları görmezden gelme', 'özel yetkilere sahip yetkili kullanıcılar tarafından alınanlar dışında, denetlenebilir olayları koruma', 'en eski kaydedilmiş denetim kayıtlarının üzerine yazma'**, 'nispeten önemsiz olarak değerlendirilebilecek denetim kayıtları arasından eski olanları silerek ek alan ayırma'**] eylemlerinden birini seçerek ve [atama: denetim belleği arızası durumunda yapılacak olan diğer eylemler] kararını alması gerekir.

Rasyonel: Bu bileşen, denetim hafızası dolduğunda denetim verilerindeki kaybın en aza indirilmesini amaçlamaktadır. Bu nedenle O.DENETİM hedefine katkı sağlar.

6.1.4. KULLANICI VERİSİNİN KORUNMASI (FDP)

FDP_ACC.1 Alt küme erişim kontrolü

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FDP_ACF.1 Güvenlik özniteliğine dayalı erişim kontrolü

FDP_ACC.1.1 TSF'nin **Erişim Kontrol Politikası**'nı (HVEKP) **[**

1. **Özneler: [atama: kullanıcı tipleri veya EKP tarafından kapsanan diğer özneler]**
2. **Nesneler:**
   a. **Şu kıstasları taşıyan veriler: [atama: verilere ilişkin kıstaslar]**
   b. **[atama: EKP tarafından kapsanan diğer nesneler]**

   İçin, söz konusu özneler ve nesneler arasındaki işlemlerde] uygulaması gerekir.

ST Yazarı Notu: Özneler ve nesneler arasındaki işlemlerin listesi; yeni bir nesnenin oluşturulması, bir nesnenin ortadan kaldırılması, bütün alternatif nesneye erişim işlemleri ve nesneyle birlikte saklanan ve nesneyle ilişkili bulunan TSF verisi üzerindeki işlemleri kapsamalıdır (örneğin nesneyle ilişkilendirilmiş erişim kontrol listesi gibi). Eğer bu işlemlerin bir kısmı TSF verisinin yönetimiyle ilgili SFR'larda tanımlanmışsa, ST yazarı, bu SFR'lara dokümanı okuyanları yönlendirecek nitelikte gerekli bilgiyi sağlamalıdır. Farklı nesneler için farklı erişim kontrol mekanizmalarının tanımlanması söz konusu olduğunda, FDP_ACC.1 bileşeni her bir farklı mekanizma için tekrar yazılarak farklı mekanizmaların tanımlanması sağlanmalıdır.

Rasyonel: Bu bileşen, veri erişim kontrolünün politikasını tanımlamaktadır. Bunu yaparken yetki bazında izinleri bir yöntem olarak kullanır. Bu nedenle O.BİLGİNİN_KORUNMASI ve O.YETKİLENDİRME hedeflerine katkı sağlar.

FDP_ACF.1 Güvenlik özniteliğine dayalı erişim kontrolü

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: FDP_ACC.1 Alt küme erişim kontrolü

FMT_MSA.3 Durağan özniteliği başlangıç durumuna getirme

FDP_ACF.1.1 TSF'nin **[**

Özne öznitelikleri:

a) Kullanıcı ID'si, kullanıcının bağlı olduğu Grup ID'si veya kullanıcıya verilen roller

b) Kullanıcının sahip olduğu roller ve yetkiler

c) Kullanıcının web sayfasına / metoda erişim talebini doğru kaynaktan doğru yöntemle yaptığından emin olunmasını sağlayacak çapraz doğrulama kodu.

d) Kullanıcıya ait session bilgileri ve istekle birlikte gönderilen parametreler

e) [atama: Özneye ait diğer öznitelikler]

Nesne öznitelikleri: Erişim Kontrol Listesi] özne ve nesneleri dikkate alınarak nesneler üzerinde **[Erişim Kontrol Politikasını]** uygulaması gerekir.

FDP_ACF.1.2 TSF'nin, kontrol edilen özneler ve kontrol edilen nesneler arasında bir işleme izin verilip verilmediğini belirlemek için aşağıdaki kuralları uygulaması gerekir: **[İşleme ancak şu durumlarda izin verilir:**

a) Bir nesne için tanımlanmış Erişim Kontrol Listesi, kullanıcı ID'sinin, kullanıcının bağlı olduğu Grup ID'sinin veya kullanıcıya verilen rolün nesneye erişimine izin veriyorsa].

FDP_ACF.1.3 TSF'nin **[Sistem_Yöneticisi rolüne sahip kullanıcılar tüm kayıt ve metodlara erişim yetkisine sahiptir]** kuralına dayalı olarak öznelerin nesnelere erişimini açık bir şekilde yetkilendirmesi gerekir.

FDP_ACF.1.4 TSF'nin **[sistemi kötüye kullandığı tespit edilen IP aralıklarından yapılan istemler veya kullanıcı ID'leri]** dayalı olarak öznelerin nesnelere erişimini açık bir şekilde reddetmesi gerekir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.BİLGİNİN_KORUNMASI ve O.YETKİLENDİRME hedeflerine katkı sağlar.

6.1.5. TANIMA VE KİMLİK DOĞRULAMA (FIA)

FIA_UID.1 Tanımlama zamanı

Hiyerarşik Bileşen(ler): Hiyerarşik bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FIA_UID.1.1 TSF'nin, kullanıcının tanımlanmasından önce kullanıcı adına yerine getirilecek olan [**TOE tarafından herkesin kullanımına açık olan sayfa, fonksiyon ve varlıklara erişim**]e izin vermesi gerekir.

FIA_UID.1.2 TSF'nin, kullanıcı adına, TSF'nin aracılık ettiği diğer tüm etkinliklere izin verilmesinden önce her bir kullanıcının başarıyla tanımlanmış olmasını gerektirmesi gerekir.

6.1.6. GÜVENLİK YÖNETİMİ (FMT)

FMT_MOF.1 Güvenlik fonksiyonları davranışının yönetimi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 Güvenlik rolleri

FMT_SMF.1 Güvenlik Fonksiyonlarının özelleştirilmesi

FMT_MOF.1.1 : TSF'nin [atama: fonksiyonların listesi] fonksiyonlarının [seçim: davranışını belirleme, davranışını yetkisiz kılma, yetki verme, değiştirme] özelliğini [atama: yetkilendirilmiş yöneticiler]'le sınırlandırması gerekir.

Rasyonel: Yetkilendirilmiş kullanıcılara güvenlik özelliklerinin yönetimini kontrol etme olanağı tanır. Bu bileşen O. YÖNETİM , O.DENETİM güvenlik hedefinin karşılanmasını amaçlamaktadır.

FMT_MSA.1 Güvenlik özelliklerinin yönetimi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: [FDR_ACC.1 Erişim kontrol alt kümesi ya da FDP_IFC.1 Bilgi akışıkontrol alt kümesi]

FMT_SMR.1 Güvenlik rolleri

FMT_SMF.1 Yönetim fonksiyonlarının belirlenmesi

FMT_MSA.1.1 : TSF'nin, güvenlik özelliklerinin [atama: güvenlik özelliklerinin listesi]'ni [seçim: varsayılan_değiştir, sorgula, değiştir, sil özelliğini [atama: yetkilendirilmiş yöneticiler]'le sınırlandırmak için [atama: **Erişim Kontrol Politikasını**, bilgi akışı kontrolü SFP(leri)]'yi uygulaması gerekir.

Rasyonel: Yetkilendirilmiş kullanıcılara güvenlik özelliklerinin yönetimini kontrol etme olanağı tanır. Bu yönetim ise güvenlik özelliklerinin izlenmesi ve değiştirilmesi için olan özellikleri içerebilmektedir. Bu bileşen O. YÖNETİM , O.DENETİM güvenlik hedefinin karşılanmasını amaçlamaktadır.

FMT_MTD.1 TSF verilerinin yönetimi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: FMT_SMR.1 Güvenlik rolleri

FMT_SMF.1 Yönetim fonksiyonlarının belirlenmesi

FMT_MTD.1.1 : TSF'nin [TSF verilerinin listesi] [varsayım_değiştir, sorgula, değiştir, sil] özelliğini [**yetkilendirilmiş yöneticiler**]'le sınırlandırması gerekir.

Rasyonel: TOE tarafından Yetkilendirilmiş kullanıcılara TSF verilerini belirtilen kurallar dahilinde yönetilmesi olanağı sağlar. Bu bileşen O. YÖNETİM güvenlik hedefinin karşılanmasını amaçlamaktadır.

FMT_SMF.1 Yönetim fonksiyonlarının belirlenmesi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FMT_SMF.1.1 : TSF'nin aşağıdaki yönetim fonksiyonlarının gerçekleştirebilmesi gerekir: [**Tablo 4 altında listelenen, TSF tarafından sağlanacak güvenlik yönetimi fonksiyonlarının listesi**].

Rasyonel: TOE tarafından yönetim fonksiyonlarının belirlenmesi gerektirir. Bu bileşen O. YÖNETİM güvenlik hedefinin karşılanmasını amaçlamaktadır.

Tablo 4: DGF Tarafından Sağlanacak Güvenlik Yönetimi Fonksiyonları Listesi

Bileşen*	**Yönetim**
FAU_SAR.1	a) Denetim kayıtlarına okuma erişim yetkisi olan kullanıcı gruplarının bakımı (silme, değiştirme, ekleme)
FAU_SEL.1	a) Denetim olaylarının görüntülenmesi/değiştirilmesi için yetkilerin bakımı
FAU_STG.3	a) Eşiğin bakımı; b) Yakın denetim depolama kesintisi durumunda alınacak eylemin (silme, değiştirme, ekleme) bakımı.
FAU_STG.4	a) Denetim depolama kesintisi durumunda alınacak eylemlerin (silme, değiştirme, ekleme) bakımı.
FDP_ACF.1	a) Açık erişim veya inkar tabanlı kararlar için kullanılan özelliklerin yönetimi
FDP_RIP.2	a) Artık bilginin korunmasının ne zaman gerçekleştirileceğinin seçiminin, DH içerisinden ayarlanabilir olması
FMT_MOF.1	a) DGF içerisindeki fonksiyonlarla etkileşen rol gruplarının yönetimi
FMT_MSA.1	a) Güvenlik özellikleri ile etkileşebilen rol gruplarının yönetimi b) Güvenlik özellikleri belirli değerlerden türemiş kuralların yönetimi
FMT_MTD.1	a) DGF verileri ile etkileşebilen rol gruplarının yönetimi
FMT_SMR.1	a) Bir rolün parçası olan kullanıcı gruplarının yönetimi
FPT_STM.1	a) Zaman yönetimi
FTA_MCS.1	a) Yönetici tarafından, izin verilen maksimum eş zamanlı kullanıcı oturum sayısının yönetilmesi

Bileşen*	Yönetim
FTA_SSL.3	a) Belirli bir kullanıcı için oluşan etkileşimli oturumun sonlandırılmasından sonra, kullanıcı hareketsizliğinin zaman özellikleri b) Etkileşimli oturumun sonlandırılmasından sonra oluşan kullanıcı hareketsizliğinin varsayılan zaman özellikleri
FTA_TSE.1	a) Kullanıcı oturumu oluşturma koşullarının yetkilendirilmiş yönetici tarafından yönetilmesi
FTP_ITC.1	a) Eğer destekleniyor ise, güvenli kanal için gerekli olayların konfigürasyonu
FTP_TRP.1	a) Eğer destekleniyor ise, güvenli yol için gerekli olayların konfigürasyonu

* FAU_GEN.1, FAU_GEN.2, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FDP_ACC.1, FMT_SMF.1, FPT_FLS.1, FRU_FLT.1, FTA_SSL.4, FTA_TAH.1 bileşenleri için öngörülen yönetim faaliyeti yoktur.

FMT_SMR.1 Güvenlik rolleri

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: FIA_UID.1 Tanımlama zamanı

FMT_SMR.1.1 : TSF'nin şu rolleri sağlaması gerekir

a) Yetkilendirilmiş Yönetici,

b) Normal Kullanıcı

FMT_SMR.1.2 : TSF'nin kullanıcıları roller ile ilişkilendirebilmesi gerekir.

Rasyonel: Farklı rollerin tanımlanması ve Kullanıcılara farklı rollerin atanabilmesini gerektirir. Bu bileşen O. YÖNETİM, O. YETKİLENDİRME YÖNETİMİ güvenlik hedefinin karşılanmasını amaçlamaktadır.

6.1.7. TSF'NİN KORUNMASI (FPT)

FPT_FLS.1 Başarısızlık durumunda güvenli durumun korunması

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Hiçbir bağımlılık yoktur.

FPT_FLS.1.1 : Aşağıdaki hata tipleri meydana geldiği zaman TSF'nin güvenilir bir durumu koruması gerekir: [atama: Uygulama Hataları, Kullanıcı Hataları].

Rasyonel: Uygulama ve yazılım hataları oluşması durumlarında bile güvenlik açısından TOE'nin doğru şekilde çalışmaya devam etmesini sağlar. Bu bileşen O. HATA_YÖNETİMİ güvenlik hedefinin karşılanmasını amaçlamaktadır.

FPT_STM.1 Güvenilir zaman etiketleri

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FPT_STM.1.1 : TSF'nin kendi kullanımı için güvenilir zaman etiketleri sağlayabilmesi gerekir.

Rasyonel: TOE içerisindeki yönetim ve denetim fonksiyonları için güvenilir bir zaman etiketi fonksiyonu sağlar . Bu bileşen O. DENETİM, OE. ZAMAN DAMGALARI güvenlik hedeflerinin karşılamasını amaçlamalıktadır.

6.1.8. HATA TOLERANSI (FRU)

FRU_FLT.1 İndirgenmiş hata toleransı

Hiyerarşiktir: Başka hiçbir öğe yoktur.

Bağımlılıklar: FPT_FLS.1 Güvenilir durumun korunduğu hata

FRU_FLT.1.1 : TSF'nin aşağıdaki hatalar meydana geldiği zaman [atama: TOE Hata Listesi]nin işletilmesini garanti etmesi gerekir: [atama: hata türlerinin listesi]

Rasyonel: TSF hata oluşması durumlarında bile güvenlik açısından TOE'nin doğru şekilde çalışmaya devam etmesini sağlar. Bu bileşen O. HATA_YÖNETİMİ güvenlik hedefinin karşılanmasını amaçlamaktadır.

6.1.9. TOE ERİŞİMİ (FTA)

FTA_MCS.1 Eşzamanlı çoklu oturumlar üzerindeki temel sınırlama

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: FIA_UID.1 Kimlik belirlemenin zamanı

FTA_MCS.1.1 : TSF'nin aynı kullanıcıya ait eşzamanlı oturumların azami sayısını kısıtlaması gerekir.

Rasyonel: TSF bir kullanıcının eş zamanlı olarak açabileceği oturum sayının güvenli bir oturum oluşturulması amacıyla kısıtlandırılmasını sağlar. Bu bileşen O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

FTA_SSL.3 TSF tarafından başlatılmış sonlandırma

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FTA_SSL.3.1 : TSF'nin [atama: kullanıcı işlemsizlik süresi] sonrasında etkileşimli bir oturumu sonlandırması gerekir.

Rasyonel: Kullanıcının işlem yapmadığı belirli bir süre sonrasında TSF'nin oturumu sonlandırması için gereksinimleri sağlar. Bu bileşen O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

FTA_SSL.4 Kullanıcı tarafından başlatılmış sonlandırma

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FTA_SSL.4.1 : TSF'nin kullanıcının kendi etkileşimli oturumunu sonlandırmasına izin vermesi gerekir.

Rasyonel: Güvenli bir oturumun kapatılması için Kullanıcıya kendi etkileşimli oturumlarını sonlandırma yeteneklerini sağlanması gerekmektedir. Bu bileşen O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

FTA_TAH.1 TOE erişim tarihi

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Bağımlılık yoktur.

FTA_TAH.1.1 : Oturumun başarıyla kurulması üzerine, TSF'nin kullanıcıya en son başarılı oturum kuruluşunun [seçim: tarih, zaman, yöntem, yer] bilgilerini görüntülemesi gerekir.

FTA_TAH.1.2 : Oturumun başarıyla kurulması üzerine, TSF'nin en son başarısız oturum kuruluşunun [seçim: tarih, zaman, yöntem, yer] bilgilerini ve en son başarılı oturum kuruluşundan itibaren başarısız denemelerin sayısını görüntülemesi gerekir.

FTA_TAH.1.3 : TSF'nin kullanıcıya bilgileri gözden geçirme fırsatını vermeden kullanıcı arabiriminden erişim geçmişi bilgilerini silmemesi gerekir.

Rasyonel: Bir kullanıcı oturum açtığında TSF'nin bu kullanıcı hesabındaki başarılı ve başarısız erişim denemelerinin tarihçesini, kullanıcıya göstermesi sağlar. Bu bileşen O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

FTA_TSE.1 TOE oturumu kurma

Hiyerarşiktir: Başka hiçbir bileşen yoktur

Bağımlılıklar: Bağımlılık yoktur.

FTA_TSE.1.1 : TSF'nin [atama: lokasyon, zaman, oturum kurma deneme sayısı]e dayanarak yetkili bir kullanıcının oturum kurulmasını reddedebilmesi gerekir.

Rasyonel: Bir kullanıcının oturumu kurma işleminin hangi durumlarda kabul edilmeyeceğini belirler. Bu bileşen O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

6.1.10. GÜVENİLİR YOLLAR/KANALLAR (FTP)

FTP_ITC.1 TSF arası güvenilir kanal

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Hiçbir bağımlılık yoktur.

FTP_ITC.1.1 : TSF'nin, kendisi ile bir başka güvenilir BT ürünü arasında, mantıksal olarak diğer iletişim kanallarından ayrı olan ve uç noktalarının kimliklerini ve kanal verilerinin değiştirme ya da açıklanmaya karşı korunmasını garanti eden bir iletişim kanalı sağlaması gerekir.

FTP_ITC.1.2 : TSF'nin [seçim: TSF, bir başka güvenilir IT ürünü]nün güvenilir kanal yoluyla iletişimi başlatmasına olanak tanıması gerekir.

FTP_ITC.1.3 : TSF'nin, güvenilir kanal yoluyla [atama: bir güvenilir kanal gerektiren fonksiyonlar listesi] için iletişimi başlatması gerekir.

Rasyonel: TSF ile diğer güvenilir BT ürünleri arasında bir iletişim gerektiğinde, iletişimin güvenilir bir kanal üzerinden yapılmasını sağlar. Bu bileşen O. BİLGİ_AKIŞI_KNTRL güvenlik hedefinin karşılanmasını amaçlamaktadır.

FTP_TRP.1 Güvenilir yol

Hiyerarşiktir: Başka hiçbir bileşen yoktur.

Bağımlılıklar: Hiçbir bağımlılık yoktur.

FTP_TRP.1.1 : TSF'nin, kendisi ile [uzak, yerel] kullanıcılar arasında, mantıksal olarak diğer iletişim yollarından ayrı olan ve uç noktalarının kimliklerini ve kanal verilerinin [seçim: değiştirme, açıklanma, [atama: diğer bütünlük ya da gizlilik ihlali türleri]]ne karşı korunmasını garanti eden bir iletişim kanalı sağlaması gerekir.

FTP_TRP.1.2 : TSF'nin, [TSF, yerel kullanıcılar, uzaktaki kullanıcılar]ın güvenilir yol üzerinden iletişimi başlatmasına olanak tanıması gerekir.

FTP_TRP.1.3 : TSF, güvenilir kanalın [başlangıçtaki kullanıcı doğrulama, yönetim fonksiyonları, veri transferi] için kullanılmasını gerektirmelidir.

Rasyonel: Kullanıcılardan TSF'ye ya da TSF'den kullanıcılara güvenilir bir iletişim oluşturulmasını ve bunun sürdürülmesini sağlar. Güvenlikle ilgili herhangi bir etkileşimde güvenilir bir erişim yolu gereklidir. Kullanıcı tarafından TSF ile etkileşim sırasında güvenli bir erişim yolu kurulmalıdır ya da TSF, güvenilir bir yolu kullanarak kullanıcıyla iletişim oluşturmalıdır. Bu bileşen O. BİLGİ_AKIŞI_KNTRL güvenlik hedefinin karşılanmasını amaçlamaktadır.

6.2. GÜVENLİK GARANTİ GEREKSİNİMLERİ

Bu Koruma Profili, OK Bölüm 3 altında yer verilen ve EAL 2 seviyesi için geçerli olan tüm Güvenlik Garanti Gereksinimlerini kapsar. Bununla birlikte aşağıdaki hususları da dikkate alır:

OK Bölüm 3 altında tanımlanan ASE_CCL.1 şu şekilde yeniden yazılmıştır: Tüm Geliştirici Eylem Elemanları, İçerik ve Sunum Elemanları, Değerlendirici Eylem Elemanları olduğu gibi korunmuştur. Ancak şu kısım yeniden yazılmıştır:

ASE_CCL.1.10C Uyumluluk bildirimi rasyonelinin tespiti ve doğrulanmasında, Koruma Profili ile belirlenen fonksiyonel güvenlik bileşenlerinde "ST Yazarı Notu" adlı alt başlıklarda (varsa) tanımlanan gereksinimler dikkate alınmalıdır.

Tablo 5'te ALC_FLR.1 ve ALC_LCD.1 ile genişletilmiş EAL 2 paketinin güvenlik garanti gereksinimleri liste halinde sunulmaktadır.

Tablo 5: Güvenlik Garanti Gereksinimleri Bileşen Listesi

Garanti Sınıfı	Garanti Bileşeni İsmi	Bileşen
ADV: Geliştirme	Güvenlik mimari tanımlaması	ADV_ARC.1
	Güvenliği zorlayan fonksiyonel belirtim	ADV_FSP.2
	Temel tasarım	ADV_TDS.1
AGD: Klavuz dokümanlar	Operasyonel kullanıcı klavuzu	AGD_OPE.1
	Hazırlık prosedürleri	AGD_PRE.1
ALC: Yaşam döngüsü desteği	Merkezi Yönetim (CM) sisteminin kullanımı	ALC_CMC.2
	DH'nin Merkezi Yönetim bileşeninin parçaları	ALC_CMS.2
	Dağıtım prosedürleri	ALC_DEL.1
	Temel kusur iyileştirme	ALC_FLR.1
	Geliştirici tanımlı yaşam döngüsü modeli	ALC_LCD.1
ASE: Güvenlik hedefi değerlendirmesi	Uyumluluk beyanı	ASE_CCL.1
	Genişletilmiş bileşenler tanımı	ASE_ECD.1
	GH giriş	ASE_INT.1
	Güvenlik hedefleri	ASE_OBJ.2
	Türemiş güvenlik gereksinimleri	ASE_REQ.2
	DH özet özellikleri	ASE_TSS.1

Garanti Sınıfı	Garanti Bileşeni İsmi	Bileşen
ATE: Testler	Kapsam kanıtı	ATE_COV.1
	Fonksiyonel test	ATE_FUN.1
	Bağımsız test - örnek	ATE_IND.2
AVA: Açıklık değerlendirme	Açıklık Analizi	AVA_VAN.2

6.3. GÜVENLİK GEREKSİNİMLERİ GEREKÇESİ

6.3.1. FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ BAĞIMLILIKLARI

Tablo 6'da, seçilen Fonksiyonel Güvenlik Gereksinimlerinin Ortak Kriterlerde belirtilen bağımlılıkları ve bu Koruma Profilinde bağımlılıkların nasıl kapsandığı verilmektedir.

Tablo 6: Fonksiyonel Güvenlik Gereksinimleri Bağımlılıkları Listesi

Bileşen	Bağımlılık	Kapsama
FAU_GEN.1	FPT_STM.1 Güvenilir zaman mühürleri	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 Denetim verilerinin oluşturulması FIA_UID.1 Kimlik belirlemenin zamanlaması	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1 Denetleme verilerinin oluşturulması	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Denetimin gözden geçirilmesi	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1 Denetimin gözden geçirilmesi	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 Denetim verilerinin oluşturulması FMT_MTD.1 DGF verisinin yönetilmesi	FAU_GEN.1 FMT_MTD.1
FAU_STG.1	FAU_GEN.1 Denetim verilerinin oluşturulması	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Korunmuş denetim takibi belleği	FAU_STG.1
FAU_STG.4	FAU_STG.1 Korunmuş denetim takibi belleği	FAU_STG.1
FDP_ACC.1	FDP_ACF.1 Güvenlik özniteliğine dayalı erişim kontrolü	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Alt küme erişim kontrolü FMT_MSA.3 Durağan özniteliği başlangıç durumuna getirme	FDP_ACC.1 FMT_MSA.1
FIA_UID.1	-	-
FMT_MOF.1	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Güvenlik Fonksiyonlarının özelleştirilmesi	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDR_ACC.1 Erişim kontrol alt kümesi ya da FDP_IFC.1 Bilgi akışı kontrol alt kümesi] FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim fonksiyonlarının belirlenmesi	FDR_ACC.1 FMT_SMR.1 FMT_SMF.1

Bileşen	Bağımlılık	Kapsama
FMT_MTD.1	FMT_SMR.1 Güvenlik rolleri FMT_SMF.1 Yönetim fonksiyonlarının belirlenmesi	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Kimlik belirlemenin zamanlaması	-
FPT_FLS.1	-	-
FPT_STM.1	-	-
FRU_FLT.1	FPT_FLS.1 Başarısızlık durumunda güvenli durumun korunması	FPT_FLS.1
FTA_MCS.1	FIA_UID.1 Kimlik belirlemenin zamanlaması	FIA_UID.1
FTA_SSL.3	-	-
FTA_SSL.4	-	-
FTA_TAH.1	-	-
FTA_TSE.1	-	-
FTP_ITC.1	-	-
FTP_TRP.1	-	-

6.3.2. GÜVENLİK GARANTİ GEREKSİNİMLERİ BAĞIMLILIKLARI

Tablo 7'de, seçilen Güvenlik Garanti Gereksinimlerinin Ortak Kriterlerde belirtilen bağımlılıkları ve bu Koruma Profilinde bağımlılıkların nasıl kapsandığı verilmektedir.

Tablo 7: Güvenlik Garanti Gereksinimleri Bağımlılıkları Listesi

Bileşen	Bağımlılık	Kapsama
ADV_ARC.1	ADV_FSP.1 Temel fonksiyonel belirtim ADV_TDS.1 Temel tasarım	ADV_FSP.1 ADV_TDS.1
ADV_FSP.2	ADV_TDS.1 Temel tasarım	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2 Güvenlik uygulayan fonksiyonel belirtim	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1 Temel fonksiyonel belirtim	ADV_FSP.1
AGD_PRE.1	-	
ALC_CMC.2	ALC_CMS.1 Değerlendirme Hedefi CM kapsamı	ALC_CMS.1
ALC_CMS.2	-	
ALC_DEL.1	-	
ALC_FLR.1	-	
ALC_LCD.1	-	
ASE_CCL.1	ASE_INT.1 ST tanıtımı ASE_ECD.1 Genişletilmiş bileşenlerin tanımı ASE_REQ.1 Beyan edilen güvenlik gerekleri	ASE_INT.1 ASE_ECD.1 ASE_REQ.1
ASE_ECD.1	-	
ASE_INT.1	-	
ASE_OBJ.2	ASE_SPD.1 Güvenlik problemi tanımı	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2 Güvenlik hedefleri ASE_ECD.1 Genişletilmiş bileşenlerin tanımı	ASE_OBJ.2 ASE_ECD.1
ASE_TSS.1	ASE_INT.1 ST tanıtımı ASE_REQ.1 Beyan edilen güvenlik gerekleri ADV_FSP.1 Temel fonksiyonel belirtim	ASE_INT.1 ASE_REQ.1 ADV_FSP.1
ATE_COV.1	ADV_FSP.2 Güvenlik uygulama fonksiyonel belirtimi ATE_FUN.1 Fonksiyonel testler	ADV_FSP.2 ATE_FUN.1
ATE_FUN.1	ATE_COV.1 Kapsamın kanıtları	ATE_COV.1
ATE_IND.2	ADV_FSP.2 Güvenlik uygulama fonksiyonel belirtimi AGD_OPE.1 Kullanıcı işletim kılavuzu AGD_PRE.1 Hazırlayıcı yöntemler ATE_COV.1 Kapsamın kanıtları ATE_FUN.1 Fonksiyonel testler	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 Güvenlik mimarisi tanımı ADV_FSP.2 Güvenlik uygulama fonksiyonel belirtimi ADV_TDS.1 Temel tasarım AGD_OPE.1 Kullanıcı işletim kılavuzu AGD_PRE.1 Hazırlayıcı yöntemler	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1

6.3.3. FONKSİYONEL GÜVENLİK GEREKSİNİMLERİ KAPSAMI

Tablo 8'de fonksiyonel güvenlik gereksinimleri ile güvenlik hedefleri arasındaki eşleşme verilmiştir. Her bir fonksiyonel güvenlik gereksinimi en az bir güvenlik hedefini kapsamakta ve her güvenlik gereksinimi de en az bir fonksiyonel güvenlik gereksinimi ile kapsanmaktadır.

Bu tablo aynı zamanda seçilen fonksiyonel güvenlik gereksinimlerinin yeterliliğini ve gerekliliğini ortaya koymaktadır.

6.3.4. EAL SEÇİMİ GEREKÇESİ

EAL seviyesi seçiminde, ürün grubunun gerektirdiği güvenlik gereksinimleri seviyesi dikkate alınmıştır. Ticari ürünler için tercih edilen EAL seviyesi, çoğunlukla EAL2 ve EAL3 olmaktadır. EAL4 ve üstü ise çoğunlukla akıllı kartlar gibi kritik BT ürünlerinde söz konusudur.

EAL seviyesinin tespitinde göz önünde bulundurulan önemli hususlardan bir diğeri ise, bu koruma profilinin kapsamında yer alan ürünlerin diğer ürün gruplarına göre daha sık güncellenme ihtiyacıdır. Çünkü bu ürün grubunda yer alan ürünlerin internet aracılığıyla erişilebilir yapısı sebebiyle güvenlik tehditleri zaman içinde değişebilmektedir. Güvenlik tehditleri değişmese bile, bu ürünlerin genellikle sıklıkla güncellemeye tabi tutulması, süreç açısından hızlı sonuç veren bir EAL derecesinin seçimini zorunlu kılmaktadır.

Tablo 8: Fonksiyonel Güvenlik Gereksinimleri Kapsamı

		Hedefler							
		O.DENETİM	O.YETKİLENDİRME	O.BİLGİ_AKIŞI_KNTRL	O.YÖNETİM	O.VERİNİN_KORUNMASI	O.HATA_YÖNETİMİ	O.ARTIK_VERİ	O. FONKSİYONEL_TEST
Fonksiyonel Güvenlik Gereksinimleri	FAU_GEN.1	✓							
	FAU_GEN.2	✓							
	FAU_SAR.1	✓			✓				
	FAU_SAR.2	✓	✓						
	FAU_SAR.3	✓			✓				
	FAU_SEL.1	✓			✓				
	FAU_STG.1	✓				✓			
	FAU_STG.3	✓			✓				
	FAU_STG.4	✓							
	FDP_ACC.1		✓			✓			✓
	FDP_ACF.1		✓			✓			
	FDP_RIP.2							✓	
	FMT_MOF.1	✓			✓				
	FMT_MSA.1	✓			✓				
	FMT_MTD.1				✓				
	FMT_SMF.1				✓				
	FMT_SMR.1		✓		✓				
	FPT_FLS.1						✓		
	FPT_STM.1	✓							
	FRU_FLT.1						✓		
	FTA_MCS.1		✓		✓				
	FTA_SSL.3		✓		✓				
	FTA_SSL.4		✓						
	FTA_TAH.1		✓						
	FTA_TSE.1		✓		✓				
	FTP_ITC.1			✓					
	FTP_TRP.1			✓					

KAYNAKLAR

20 Critical Security Controls, version 4.1, SANS Institute, (çevrimiçi) <http://www.sans.org/critical-security-controls/> (son erişim: 10 Aralık 2013)

OWASP Top 10 - 2013: The Ten Most Critical Web Application Security Risks, The Open Web Application Security Project (OWASP), 2013, (çevrimiçi) <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project> (son erişim: 10 Aralık 2013)

Web Application Security Consortium, (çevrimiçi) <http://www.webappsec.org> (son erişim: 10 Aralık 2013)