Sağlık Bilgi Sistemi Yazılımları Koruma Profili

TÜRK STANDARDLARI ENSTİTÜSÜ

ARALIK 2013

İçindekiler Tablosu

1. Koruma Profiline Giriş 4
1.1. Koruma Profili Referansı 4
1.2. Amaç ve Kapsam 4
1.3. Değerlendirme Hedefine (TOE) Genel Bakış 5
1.3.1. Giriş 5
1.3.2. Değerlendirme Hedefi Türü 5
1.3.3. Çalışma Ortamı Bileşenleri 5
1.4. Değerlendirme Hedefinin Detaylı Açıklanması 6
1.4.1. Yazılım ve Donanım Çevre Birimleri 6
1.4.2. Ana Güvenlik ve Fonksiyonel Özellikler 7
1.5. Belgeye Genel Bakış 7
2. Uyumluluk İddiaları 8
2.1. Ortak Kriterler Uyumluluk İddiası 8
2.2. Koruma Profili Uyumluluk İddiası 8
2.3. Paket Uyumluluk İddiası 8
2.4. Uyumluluk İddiası Gerekçesi 8
2.5. Uyumluluk Beyanı 8
3. Güvenlik Probleminin Tanımı 8
3.1. Giriş 8
3.2. Varlıklar 8
3.3 Tehditler 9
3.3.1. Tehdit Kaynakları (Aktörler) 9
3.3.2. Tehditler 9
3.4. Kurumsal Güvenlik Politikaları 10
3.5. Varsayımlar 10
3.5.1 Personel ile ilgili varsayımlar: 11
3.5.2 Fiziksel ortamla ilgili varsayımlar: 11
3.5.3 Bağlantı ile ilgili varsayımlar 11
4. Güvenlik Hedefleri 11
4.1. Giriş 11
4.2. Değerlendirme Hedefi için Güvenlik Hedefleri 11
4.3. Çalışma Ortamı için Güvenlik Hedefleri 12
4.4. Güvenlik Hedefleri Gerekçesi 13
4.4.1. Güvenlik Hedeflerinin Kapsamı 13
4.4.2. TOE için Güvenlik Hedeflerinin Gerekçesi 14

4.4.3. Çalışma Ortamı için Güvenlik Hedeflerinin Gerekçesi 15
5. Genişletilmiş Bileşenler Tanımı 15
6. Güvenlik Gereksinimleri 15
6.1. Fonksiyonel Güvenlik Gereksinimleri 15
6.1.1. Genel Bakış 15
6.1.2. Fonksiyonel Güvenlik Politikaları 16
6.1.3. Güvenlik Denetimi (FAU) 16
6.1.4. Kullanıcı Verisinin Korunması (FDP) 21
6.1.5. Tanıma ve Kimlik Doğrulama (FIA) 22
6.1.6. Güvenlik Yönetimi (FMT) 25
6.1.7. TSF'nin korunması (FPT) 28
6.1.8. Hata toleransı (FRU) 28
6.1.9. TOE erişimi (FTA) 29
6.1.10. Güvenilir yollar/kanallar (FTP) 30
6.2. Güvenlik Güvence Gereksinimleri 30
6.3. Güvenlik Gereksinimleri Gerekçesi 31
6.3.1. Fonksiyonel Güvenlik Gereksinimleri Bağımlılıkları 31
6.3.2. Güvenlik Güvence Gereksinimleri Bağımlılıkları 32
6.3.3. Fonksiyonel Güvenlik Gereksinimleri Kapsamı 33
6.3.4. EAL Seçimi Gerekçesi 33
Kaynaklar 35

1. Koruma Profiline Giriş

1.1. Koruma Profili Referansı

Aşağıdaki tabloda, koruma profiline ait referans bilgileri yer almaktadır.

Belge Sürümü	1.0
Yayınlanma Tarihi	
Geliştiriciler	Türk Standartları Enstitüsü
Uyum Sağlanan EAL	EAL2

1.2. Amaç ve Kapsam

Son yıllardaki gelişmeler doğrultusunda yeni bilgi teknolojileri cihazları ile yazılımları geliştirilmiş ve farklı alanlarda uygulamaya alınmıştır. Söz konusu teknolojik ürünlerin kullanılmaya başlandığı alanlardan biri de sağlık sektörüdür. Sağlık kurumlarındaki verilerin ve kaynakların etkin bir şekilde kullanılması amacıyla günümüzde çeşitli uygulama yazılımları kullanılmaktadır. Bu uygulama yazılımlarının arasında Hastane Bilgi Yönetim Sistemi (HBYS), Aile Hekimliği Bilgi Sistemi (AHBS), Görüntü Arşivleme ve İletişim Sistemi (PACS), Laboratuvar Bilgi Yönetim Sistemi (LBYS), Elektronik Belge Yönetim Sistemi (EBYS) ve buna benzer internet üzerinden servis sunan diğer sağlık bilişimi uygulama yazılımları önemli yer tutar. Bu yazılımların farklı ulusal veri tabanları ile iletişim halinde olması gerektiğinden dolayı söz konusu yazılımlar genellikle web tabanlı olarak tasarlanmakta ve geliştirilmektedir. Bu koruma profilinde web üzerinden çalışan sağlık bilgi sistemleri yazılımlarının güvenlik gereksinimleri ele alınmıştır.

Web tabanlı Sağlık Bilgi Sistemleri'ne yönelik olarak hazırlanmış olan bu koruma profilinin oluşturulma amacı, kamu ve özel hastanelerde kullanılan yazılım ürünlerine yönelik asgari güvenlik gereksinimlerinin tanımlanmasıdır.

Teknolojideki gelişmelere paralel olarak insan sağlığı ile ilgili her türlü bilgiyi barındırıp işleyen sağlık bilgi sistemleri yazılımları web tabanlı olarak geliştirilmeye başlanmıştır. Bu yazılımların internetin de yaygınlaşması ile birbiri ile bilgi alışverişi yapma ihtiyaçları doğmuştur. İnternetin tehditlere açık yapısı göz önünde bulundurulursa, söz konusu yazılımların güvenlik önlemlerinin ön plana çıkarılması ve yazılımlarda yeterli seviyede güvenlik önlemi alınması ihtiyacı ön plana çıkar. Kuruluşların söz konusu güvenlik önlemlerini etkin ve gerektiği şekilde almalarının temin edilmesi, ancak standartlara uyum ve ilgili sertifikasyonların hayata geçirilmesiyle mümkündür. Bu koruma profilinin yazılma amacı, web tabanlı sağlık bilgi sistemi uygulamalarına yönelik böylesi bir sertifikasyon mekanizmasında yol gösterici bir belgenin oluşturulması ihtiyacıdır. Bu koruma profilinde sağlık bilgi sistemleri uygulamaları ile ilgili orta seviye güvenlik önlemleri ele alınmıştır.

Koruma profili genel olarak web tabanlı sağlık bilgi sistemleri uygulamalarına yönelik olarak hazırlanmıştır. Başka bir deyişle, tüm web tabanlı sağlık bilgi sistemleri 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 tabanlı sağlık bilgi sistemi uygulaması olarak nitelendirilebilecek ürün grupları için yazılacak koruma profillerinde bu koruma profiline atıf yapılmasıdır.

Bir koruma profili hazırlanırken, uygulamanın korumakla yükümlü olduğu verinin kritiklik ve gizlilik derecesi, veri kaybında, izinsiz değiştirilmesinde veya sızdırılmasında ortaya çıkacak maddi veya manevi zararın büyüklüğü gibi hususlar da dikkate alınmalıdır. Bu çalışmaya konu olan uygulamalarda hastalara ait sağlık bilgileri tutulmaktadır. Bunun yanında sağlık sektörü çalışanlarının kişisel bilgileri de (görevli hekim, görevli olduğu sağlık birimleri, muayenede bulunduğu hastalar, vb.) uygulamalarda yer almaktadır. Söz konusu verilerin gerek kişisel anlamda gerekse de istatistiki anlamda yanlış kişilerin eline geçmesi durumunda onarılması güç hasarlara neden olabilir. Bu nedenle TOE'nin güvenliği sağlanmadığında ortaya çıkabilecek maddi ve manevi kayıplar ciddi seviyelere ulaşabilir. Bunun da ötesinde ortaya çıkabilecek prestij kaybı da işin başka bir boyutunu göstermektedir. Bu nedenle gerek kamudaki gerekse de özel sektördeki sağlık birimleri için uygulamalarda güvenliğin sağlanması elzemdir.

1.3. Değerlendirme Hedefine (TOE) Genel Bakış

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

1.3.1. Giriş

TOE, bir web tabanlı Sağlık bilgi yönetim sistemi uygulamasıdır. Burada bahsedilen web tabanlı sağlık bilgi sistemi kavramı ile kullanıcıların internet üzerinden erişim sağladıkları, her türlü hasta verisini işleyen ve saklayan uygulamalar kastedilmektedir.

Bu koruma profili, sağlıkla ilgili her türlü veriyi işleyip depolayabilen; Hastane Bilgi Yönetim Sistemi (HBYS), Aile Hekimliği Bilgi Sistemi (AHBS), Görüntü Arşivleme ve İletişim Sistemi (PACS), Laboratuvar Bilgi Yönetim Sistemi (LBYS), Elektronik Belge Yönetim Sistemi (EBYS) ve internet üzerinden servis sunan diğer sağlık bilişimi uygulama yazılımları için hazırlanmış genel bir koruma profilidir. Bu nedenle bu koruma profilinde yukarıda bahsedilen uygulamalarda ortak olarak bulunan güvenlik fonksiyonel özellikleri dikkate alınarak hazırlanmıştır.

1.3.2. Değerlendirme Hedefi Türü

TOE türü, web tabanlı sağlık bilgi sistemi uygulamasıdır. TOE burada hasta değerlendirmelerinin, tetkiklerinin, kullanılan ilaçların ve diğer ilgili materyallerin, giriş ve değerlendirme tarihlerinin, ilgili raporlamaların kayıtlarını tutar ve gerektiğinde yeniden erişilmesini sağlayarak yeniden kullanılmalarına olanak sağlar. Bu sayede TOE aynı zamanda hastaların başvurularını müteakip olarak hemen inceleme yapılmasına da olanak sağlar. Bunun yanında TOE hastalara ait kişisel bilgiler (Hasta adı, soyadı, Doğum tarihi/Doğum yeri, Kan grubu gibi) ile hastanın iletişim bilgileri (Sosyal Güvenlik Numarası, T.C. Kimlik Numarası, vb) ile hastanın geçirdiği ameliyat bilgilerini de güvenli olarak saklar.

TOE aynı zamanda hasta bilgileri güvenliğini sağlamak amacıyla kimlik doğrulama, erişim kontrolü, güvenli iletişim ve güvenlik yönetimi gibi temel güvenlik işlevlerini de sağlar.

1.3.3. Çalışma Ortamı Bileşenleri

TOE, bir ağ üzerinde çalışması sebebiyle ağ bileşenleriyle etkileşim halindedir. TOE'nin üzerinde çalıştığı bir web sunucusu, bu web sunucusunun üzerinde çalıştığı bir işletim sistemi, bu işletim sisteminin

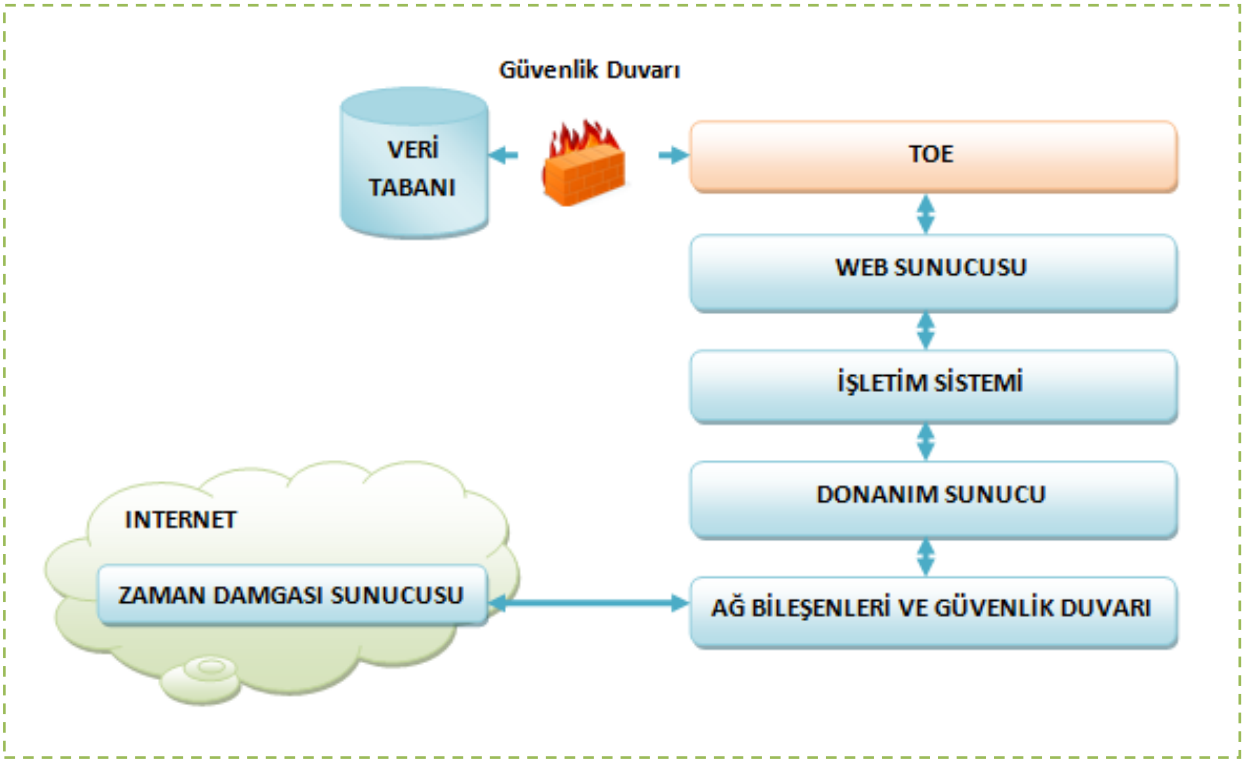
de üzerinde çalıştığı bir donanımsal sunucu bulunmaktadır. Bu bileşenler Madde 1.4.1 de detaylı bir şekilde açıklanmaktadır.

1.4. Değerlendirme Hedefinin Detaylı Açıklanması

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. Yazılım ve Donanım Çevre Birimleri

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.



Şekil 1 – TOE çalışma ortamının genel yapısı

Web Sunucusu: TOE bir web uygulaması olarak bir web sunucusu üzerinde çalışmaktadır. Bu web sunucusu herhangi bir teknolojiyi kullanıyor olabilir.

İşletim Sistemi: TOE'nin üzerinde çalıştığı sunucunun bir işletim sistemi bulunmaktadır. TOE'nin üzerinde çalıştığı web sunucusu bu işletim sistemi üzerinde çalışmakta ve sistem kaynaklarını bu işletim sistemi vasıtasıyla kullanmaktadır.

Donanımsal Sunucu: TOE donanımsal olarak bir sunucu üzerinde çalışmaktadır. Söz konusu sunucu üründen ürüne farklı özellikler gösterebilir.

Ağ Bileşenleri ve Güvenlik Duvarı: TOE, hasta bilgilerinin paylaşılması ve diğer bilgi paylaşımları için ağ bileşenleriyle etkileşim halindedir. Bu etkileşim, işletim sistemi ve sunucu aracılığıyla gerçekleştirilir. TOE'nin internet erişimi, bir güvenlik duvarı tarafından denetlenmektedir.

Zaman Damgası Sunucusu: TOE, işlem kayıtlarının güvenliğini sağlamak amacıyla çalışma ortamı tarafından sağlanan zaman damgasına ihtiyaç duyar. Bu zaman damgası, donanımsal olarak üretilen elektronik imza tabanlı olma özelliklerine sahiptir.

Veritabanı : TOE'nin tüm kullanıcı ve hasta verilerini sakladığı veritabanıdır. Önünde bir güvenlik duvarı yer alır.

1.4.2. Ana Güvenlik ve Fonksiyonel Özellikler

TOE'nin güvenlikle ilgili özellikleri aşağıda verilmiştir:

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

Kontrollü Erişim: TOE, sağlanan kullanıcı adı ve parolalarına göre önceden yetkilendirilmiş kaynaklara erişim izni sağlar. Hangi kullanıcının hangi bilgi kaynaklarına erişebileceği ile ilgili bilgiler Erişim Denetimi Listeleri'nde tutulur.

Kayıt Tutma: TOE, sistemdeki varlıklar üzerindeki kullanıcı faaliyetlerinin, erişim kontrolü ve değişiklik kayıtlarının tutulabilmesi amacıyla otomatik olarak denetim kayıtlarını tutar. Denetim kayıtlarının içeriği ve tutulma yöntemi kolay anlaşılabilir bir formatta olmalı ve TOE tarafından sunulan arayüz üzerinden ayarlanabilmelidir. TOE, kayıtların değiştirilmesine karşı, tuttuğu işlem kayıtlarını zaman damgası ile damgalar. İşlem kayıtlarının yetkisiz değiştirilmesi TOE tarafından tespit edilebilir.

Yönetim: Sistemin yönetiminden sorumlu kullanıcılara, TOE tarafından etkin yönetim mekanizmaları sunulur. Bu mekanizmaların hızlı ve etkin karar almayı kolaylaştırması önem taşımaktadır. Sistem yönetiminden sorumlu kullanıcılara yetkilendirme yönetimi ve veri yönetimi fonksiyonellikleri sağlanır. TOE'nin yönetimi için sağlanan arayüzler yalnızca özel yetki verilmiş kişilerin erişimine açık olup, diğer arayüzlere göre daha sıkı güvenlik önlemlerine tabi tutulur. TOE için tanımlanmış olan roller asgari olarak yönetici, kullanıcı ve denetçi rolleridir. Yönetici rolü, TOE'nin yönetimi ile ilgili fonksiyonları gerçekleştiren roldür. Kullanıcı rolü TOE yi yetkisi dâhilinde kullanan roldür. Denetçi rolü ise, sistemde denetim yapmak amacıyla sadece denetim fonksiyonlarını (yapılandırma ayarları, kayıtlara bakma vb.) kullanabilen roldür.

Veri Koruması: TOE tarafından temel olarak hasta verileri ve kullanıcı verileri olmak üzere iki tür veri tutulur. TOE söz konusu verileri korumakla yükümlüdür. Bu verilerin korunması TOE'nin sorumluluğundadır. Veri korunmasının sadece verinin saklanması esnasında değil, aynı zamanda veri iletimi esnasında da sağlanması gerektiğine dikkat edilmelidir.

1.5. Belgeye Genel Bakış

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

Bölüm 5'te güvenlik hedeflerini sağlayacak fonksiyonel ve güvence gereksinimlerini de içerecek şekilde güvenlik gereksinimleri açıklanmaktadır.

Bölüm 6'da Güvenlik gereksinimleri ana başlığı altında Güvenlik fonksiyonel gereksinimleri, Güvenlik Güvence Gereksinimleri ve Güvenlik Güvence Gereksinimlerinin gerekçeleri ele alınmıştır.

Son bölüm olan Kaynaklar bölümünde kayda değer görülen destekleyici kaynaklara yer verilmektedir.

2. Uyumluluk İddiaları

2.1. Ortak Kriterler Uyumluluk İddiası

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

Bu koruma profili OK Bölüm 2 ile tam uyuma sahiptir.

Bu koruma profili, OK Bölüm 3 ile tam uyuma sahiptir.

2.2. Koruma Profili Uyumluluk İddiası

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

2.3. Paket Uyumluluk İddiası

Bu Koruma Profili, Ortak Kriterler Bölüm 3 altında tanımlanan güvence paketlerinden EAL 2 ile uyumludur.

2.4. Uyumluluk İddiası Gerekçesi

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

2.5. Uyumluluk Beyanı

Bu Koruma Profili, "tam uyumluluk" gerektirmektedir.

3. Güvenlik Probleminin Tanımı

3.1. Giriş

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. Varlıklar

Çizelge 1: Varlıklar	
Tanım	**Açıklama**

V.Kullanıcı_Verisi	TOE'yi kullanan kullanıcılara ait kişisel bilgiler (Doktor, hemşire, sistem yöneticisi, veri giriş operatörü vb. kullanıcılara ait isim soyisim, Kimlik No, İletişim bilgileri gibi bilgiler)
V.Hasta_Verisi	TOE tarafından işlenen ve depolanan hassas niteliğe sahip hasta bilgileri (Hastalık türü, hastanın durumu, hastalığın seyri, hastaya yapılan tıbbi işlemler, hastaya ait kişisel bilgiler vb.)
V.Kimlik_Doğrulama_Verisi	Yetkili kullanıcıların TOE fonksiyonlarına erişim için kullandıkları kullanıcı adı/parola bilgileri
V. Sistem Verisi	Sistemde tutulan yapılandırma ve işlem kayıt verileri

3.3 Tehditler

3.3.1. Tehdit Kaynakları (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.

3.3.2. Tehditler

T.YETKİSİZ_ERİŞİM	Yetkisiz bir kullanıcı ya da saldırgan, erişim izni bulunmayan verilere herhangi bir yöntemle erişmeye çalışabilir. Erişim sağlaması durumunda ise hassas verileri (**V.Hasta_Verisi, V.Kullanıcı_Verisi, V.Kimlik_Doğrulama_Verisi, V.Sistem_Verisi**) ele geçirebilir ya da bu verileri değiştirebilir. Bu durum bilginin sızdırılmasına, bilgi bütünlüğünün bozulmasına ve bilginin güvenilirliğin kaybolmasına neden olur. Varsayılan kullanıcı adları ve parolaların değiştirilmemesi, basit parolaların kullanımı, test hesaplarının aktif sistemde de bulunması gibi güvenlik açıklarından faydalanan Saldırgan, TOE'ye yetkisiz erişim sağlayabilir
T.YANILTMA	Saldırgan, yetkili TOE kullanıcısını farklı bir adrese yönlendirerek kullanıcının kimlik/parola bilgilerini ele geçirmek için teşebbüste bulunabilir. Bu teşebbüs, sahte bir IP adresi veya etki alanı adı ve TOE ye benzer bir arayüz kullanılarak yapılabilir. Bu tehdide örnek olarak yetkili Kullanıcı veya Sistem_Yöneticisinin, Saldırgan tarafından uygulamanın bulunduğu adresten farklı bir adrese yönlendirilerek ve bu adresin TOE'ye ait olduğu izlenimi edinmeleri sağlanarak, sisteme erişim için kullandıkları bilgilerin (**V_Kimlik_Doğrulama_Verisi**) ele geçirilmesi verilebilir.
T.VERİ_DEĞİŞTİRME	TOE tarafından korunan bir veri, yetkisiz kişilerce izinsiz olarak değiştirilebilir. Örneğin Saldırgan; TOE ile TOE'nin çalışma ortamı bileşenleri arasındaki ağ üzerinde taşınan bilgiyi (**V.Hasta_Verisi, V.Kullanıcı_Verisi, V.Sistem_Verisi**) izinsiz olarak değiştirebilir veya saldırgan TOE ye eriştikten sonra, işlem kayıtlarını değiştirerek izini kaybettirmek isteyebilir. Veri aktarımı esnasında veri bütünlüğünün temin edildiği protokollerin tercih edilmemesi veya hassas kayıtların bütünlüğünün sağlanmaması bu tehdidin gerçekleşmesini kolaylaştırmaktadır.
T.VERİ_SIZDIRMA	TOE tarafından korunan kullanıcı (**V.Kullanıcı_Verisi**) veya hasta verilerinin (**V.Hasta_Verisi**) yetkisiz olarak sızdırılmasıdır. 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 tehdidin gerçekleşmesini kolaylaştıran bir husustur. Bu tür tehditler genellikle TOE nin çalıştığı iç ağdan kolaylıkla gerçekleştirilebilmektedir.
T.MAHREMİYET	TOE tarafından korunan hasta ve kullanıcı verilerinin (**V.Hasta_Verisi ve V.Kullanıcı_Verisi**) yetkili bir kullanıcı tarafından TOE'nin fonksiyonları kullanılarak ifşa edilmesidir. Örneğin yetkili bir kullanıcı yetkisi dâhilinde genel istatistiki bir rapor alırken, hastaların kimliklerini tanımlayan verilerin de raporda yer alması bu kapsamda değerlendirilebilir. Özellikle hassas nitelikteki verilerin açık şekilde saklanması bu tehdidin gerçekleşmesini kolaylaştıran bir husustur.
T.HİZMET_AKSATMA	TOE'nin sağladığı bir hizmetin veya TOE sistemin bir süreliğine kullanılamaz veya erişilemez hale getirilmesi tehdididir. Örneğin Saldırgan, TOE'ye sürekli ve yoğun talepte bulunarak TOE'nin bunlara cevap veremez hale gelmesini sağlayabilir. Hizmet aksatmanın bir ileri seviyesi olan dağıtık hizmet aksatma saldırıları, ayrıca değerlendirilmesi gereken tehditlerdir. Bu tehditlerin engellenmesi amacıyla TOE üzerinde bazı tedbirler alınabilse de, bu tehditlerin engellenmesi için genellikle yazılım katmanında alınan önlemler yeterli olmaz.
T.YETKİ_YÜKSELTME	Yetki yükseltmesi, sınırlı yetkilere sahip bir kullanıcının daha yetkili bir kullanıcının yetkilerini alması durumudur. Saldırgan, T.YANILTMA tehdidiyle ilgili yöntemleri kullanarak sisteme erişim sağlayıp, daha sonra yetki yükseltmesi ile daha üst seviye bir yetkiye sahip olabilir. Bu sayede saldırgan hassas **V.Hasta_Verisi** ile **V.Sistem_Verisi**'ne erişim sağlayabilir.
T.KÖTÜCÜL_GÜNCELLEME	Saldırgan, TOE'nin güvenlik fonksiyonlarını değiştirmek için TOE yazılımını kötücül bir yazılım ile güncellemeye çalışabilir. Bu sayede saldırgan **V.Sistem _Verisi'ni** değiştirebilir ve/veya bir gizli kanal vasıtasıyla **V.Hasta_Verisi** ve **V.Kullanıcı_Verisi**'ni ele geçirebilir.
T.GÜNLÜK_BOZMA	Saldırgan, güvenlikle alakalı olarak günlük kayıtlarının tutulması fonksiyonunu devre dışı bırakabilir(örneğin depolama alanını yetersiz bırakarak). Saldırgan, TOE tarafından tutulan işlem kayıtlarına hatalı kayıtlar ekleyerek veya silerek **V.Sistem_Verisi**'ne duyulan güveni azaltabilir veya Sistem Yöneticisini sorunların çözümünde yanlış yönlendirebilir.

3.4. Kurumsal Güvenlik Politikaları

Bu koruma profili kapsamında herhangi bir kurumsal güvenlik politikası tanımlanmamıştır.

3.5. Varsayımlar

Web uygulamalarına yönelik olan bu koruma profili hazırlanırken yapılmış olan varsayımlar üç ana başlıkta toplanmıştır.

- ✓ Personel ile ilgili varsayımlar

- ✓ Fiziksel ortamla ilgili varsayımlar
- ✓ Bağlantı ile ilgili varsayımlar

3.5.1 Personel ile ilgili varsayımlar

A.GÜVENİLİR_YÖNETİCİ	TOE ve TOE'nin bulunduğu ortam üzerindeki BT varlıklarının kurulum, konfigürasyon ve işletim görevlerinden sorumlu tüm kullanıcıların Tecrübeli ve eğitimli oldukları ve güvenlik tarama şartlarını sağladıkları varsayılmaktadır.

3.5.2 Fiziksel ortamla ilgili varsayımlar

A.FİZİKSEL_GÜVENLİK	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.

3.5.3 Bağlantı ile ilgili varsayımlar

A.GÜVENLİ_İLETİŞİM	TOE'nin etkileşim içinde olduğu uzak BT sistemleri ile yaptığı ve TSF tarafından korunmayan TSF'nin fiziksel olarak ayrı bölümlerinin kendi aralarında yaptıkları tüm iletişim ve iletişimin yapıldığı ağın çeşitli saldırılara (Dağıtık Hizmet Aksatma saldırıları, Ağ'a sızma girişimleri, kötücül yazılım bulaştırma saldırıları vb.) karşı, güvenliğinin sağlandığı varsayılmaktadır. Bu kapsamda iletilen verilerin bütünlük ve gizliliğinin sağlandığı ve iletişim uç noktalarının kaynağının doğrulandığı da varsayılmaktadır. Güvenli iletişim web üzerinde yaygın olarak SSL bağlantı ile https protokolü ile sağlanmaktadır. Uygulama Notu: TOE ayrı bölümlerden oluşuyor ve TOE bu bölümler arasında iletilen TSF verisinin korunmasını sağlayan mekanizmalar uyguluyor ise, ST yazarı, A.GÜVENLİ_İLETİŞİM'i desteklemek veya kaldırmak için FPT_ITT.1 i kullanmayı seçebilir.

4. Güvenlik Hedefleri

4.1. Giriş

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

Güvenlik hedefleri, TOE için Güvenlik Hedefleri (TOE tarafından doğrudan 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. Değerlendirme Hedefi için Güvenlik Hedefleri

O. KAYIT_TUTMA	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 izlenmeli ve gerektiğinde bu kayıtlar üzerinde inceleme yapılabilmesine

	olanak sağlanmalıdır.
O.KİMLİK_DOĞRULAMA	TOE, sistemde tanımlı olan tüm kullanıcıların tekil ve benzersiz olarak tanımlanmasını sağlamalı ve sisteme erişim izni vermeden önce kullanıcının kimliğini doğrulamalıdır.
O. YETKİLENDİRME	TOE, sistemde tanımlı olan tüm kullanıcıları her birinin birbirinden farklı olarak tanımlanmasını sağlamalı ve farklı seviyelerle yetkilendirebilmelidir. TOE sisteme erişimde kullanıcının yetkisini kontrol etmeli ve bu yetkiye göre erişim olanağı sağlamalıdır.
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 içeriği kontrol edilmelidir.
O. YÖNETİM	TOE, TOE 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.
O. BİLGİ_KORUMA	TOE, sistem üzerindeki verilerinin yetkisiz olarak görüntülenmesi, değiştirilmesi ve silinmesine karşı gerekli güvenlik önlemlerini sağlamalıdır.
O.MAHREMİYET	TOE, sistem üzerindeki hasta verilerinin yetkili fakat gereksiz olarak görüntülenmesi ve kopyalanmasına karşı gerekli güvenlik önlemlerini sağlamalıdır.
O. HATA_YÖNETİMİ	TOE, sistem üzerinde hata yönetiminin yapılmasını, doğru süreçlerin çalıştırılmasını sağlamalıdır. TOE tarafından oluşabilecek tüm hata durumları yönetilmeli ve kullanıcılara bu hatalar daha güvenli ve anlamlı hale getirilerek gösterilmelidir.
O.GÜNCELLEME	TOE, üretici tarafından imzalanan güncelleme paketinin imzasını doğrulamalı ve bu sayede yetkisiz güncellemelerin önüne geçmelidir.

4.3. Çalışma Ortamı için Güvenlik Hedefleri

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_YÖNETİCİ	TOE çalışma ortamı güvenlik hedefleri, TOE çalışma ortamı üzerinde yetkili tüm kullanıcıların gerekli eğitim almış ve tüm güvenlik gereksinimlerini sağlamış olmaları sağlamalıdır.
OE. DENETİM_VE_İZLEME	TOE'nin bulunduğu çalışma ortamına yapılan tüm giriş-çıkışların kontrol altında tutulması ve kayıt altına alınması gerekmektedir. Bu kayıtların sürekli olarak izlenmeli ve gerektiğinde bu kayıtlar üzerinde inceleme yapılabilmesine olanak sağlanmalıdır.
OE. ZAMAN DAMGASI	TOE çalışma ortamı güvenlik hedefleri, güvenlikle ilgili olay kayıtlarını zamanlarının yeterince hassas olarak kaydedilmesi için zaman damgalarının oluşturmasını sağlamalıdır. Oluşturulan zaman damgası,

elektronik imza tabanlı olmalıdır.

OE. GÜVENLİ_İLETİŞİM	TOE çalışma ortamı TOE için güvenli bir iletişim ortamı sağlamalıdır. Güvenli iletişim ortamı ağ güvenliği tedbirleri alınarak sağlanmalıdır.

4.4. Güvenlik Hedefleri Gerekçesi

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

Güvenlik hedeflerinin gerekçesi;

- 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 varsayım kapsamaktadır.

4.4.1. Güvenlik Hedeflerinin Kapsamı

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									Varsayımlar		
		T.YETKİSİZ_ERİŞİM	T.YANILTMA	T.VERİ_DEĞİŞTİRME	T.VERİ_SIZDIRMA	T.MAHREMİYET	T.HİZMET_AKSATMA	T.YETKİ_YÜKSELTME	T.KÖTÜCÜL_GÜNCELLEME	T.GÜNLÜK_BOZMA	A.GÜVENİLİR_YÖNETİCİ	A.FİZİKSEL_GÜVENLİK	A.GÜVENLİ_İLETİŞİM
Güvenlik Hedefleri	O. KAYIT_TUTMA				X			X		X			
	O.KİMLİK_DOĞRULAMA	X		X									
	O. YETKİLENDİRME		X	X				X					
	O. BİLGİ_AKIŞI_KNTRL			X	X				X				
	O. YÖNETİM			X									
	O. BİLGİ_KORUMA	X		X	X			X					
	O.MAHREMİYET					X							
	O. HATA_YÖNETİMİ				X			X					
	O.GÜNCELLEME								X				
Çalışma Ortamı Güv. Hed.	OE. FİZİKSEL GÜVENLİK											X	
	OE. GÜVENİLİR_YÖNETİCİ										X		
	OE. DENETİM_VE_İZLEME											X	
	OE. ZAMAN DAMGASI			X						X			
	OE. GÜVENLİ_İLETİŞİM						X						X

4.4.2. TOE için Güvenlik Hedeflerinin Gerekçesi

TOE GÜVENLİK HEDEFİ	GEREKÇESİ
O. KAYIT_TUTMA	TOE, sistem fonksiyonlarına erişim ve güvenlik ile ilgili yapılan işlemlerin tamamının kayıt altına alınmasını sağlar. Bu kayıtların güvenli bir şekilde korunmasına ve gerektiğinde bu kayıtların izlenmesine olanak verir. TOE tarafından, denetim verisi dolması durumunda aksiyon alınması için bir fonksiyon sağlanır. Denetim verisinin üretilmesi, ardışık kimlik doğrulama girişimleri sırasında TOE'nin denetim verisini kullanarak saldırganın kimliğini tespit edebilmesini sağlar. Denetim kayıtları, sahte kimlik kullanım ile yanıltma, belirli bir işlem ya da işlemler bütününün inkar edilmesi, hizmetin veya sistemin engellenmesi, izinsiz yetki yükseltmesi ve günlüklerin kötü kullanımı gibi güvenlik sorunlarını engeller. Bu nedenle, T.VERİ_SIZDIRMA, T.YETKİ_YÜKSELTME, T.GÜNLÜK_BOZMA tehditlerine karşı önlem sağlar.
O.KİMLİK_DOĞRULAMA	Bu güvenlik hedefi, TOE'nin erişim izni vermeden önce kullanıcının doğrulanmasını sağlar. Kimlik doğrulama işlemi genellikle kullanıcı adı/parola sorgulaması ile yapılır. Ancak bazı özel uygulamalarda bu işlem biyometrik sistemler kullanılarak da yapılabilir. 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 güvenlik hedefi ile sağlanan kimlik doğrulama mekanizması, sisteme yetkisiz erişimlerin engellenmesini ve dolayısı ile de veri bütünlüğünün korunmasını sağlayacaktır. Bu nedenle bu güvenlik hedefi; T.YETKİSİZ_ERİŞİM ve T.VERİ_DEĞİŞTİRME tehdidine karşı önlem sağlar.
O. YETKİLENDİRME	Bu güvenlik hedefi kullanıcıların yetkilendirilmesini sağlar. Bu işlem 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. Bu nedenle, T.YANILTMA, T.VERİ_DEĞİŞTİRME ve T.YETKİ_YÜKSELTME tehditlerine karşı önlem sağlar.
O. BİLGİ_AKIŞI_KNTRL	Bu güvenlik hedefi, 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_DEĞİŞTİRME, T.VERİ_SIZDIRMA ve T.KÖTÜCÜL_GÜNCELLEME 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_DEĞİŞTİRME tehditlerini karşı önlem sağlar.
O. BİLGİ_KORUMA	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_DEĞİŞTİRME, T.VERİ_SIZDIRMA, T.YETKİSİZ_ERİŞİM ve T.YETKİ_YÜKSELTME tehditlerine karşı önlem sağlar.
O.MAHREMİYET	Bu güvenlik hedefi, sistem üzerindeki hasta verilerinin yetki dâhilinde ve gereksiz şekilde görüntülenmesini ve kopyalanmasına karşı gerekli güvenlik önlemlerini sağlar. Bu nedenle, T.MAHREMİYET tehdidine 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 engellenmesi sağlanır. Bu

	nedenle, T.VERİ_SIZDIRMA ve T.YETKİ_YÜKSELTME tehditlerine karşı önlem sağlar.
O.GÜNCELLEME	Geliştirilmiş bir TOE üzerinde zaman zaman güncellemelerin yapılması gerekli olabilir. Söz konusu güncellemeler üretici tarafından imzalanan güncelleme paketleri vasıtası ile yapılmalıdır. TOE bu güncelleme paketlerinin güvenilirliğini doğrulamalı ve yetkisiz güncellemelerin önüne geçmelidir. Yetkisiz varlıklarca yapılabilecek kötü niyetli güncellemeler sistemin bütünlüğüne zarar verebilir ve veri kaybına neden olabilir. Bu güvenlik hedefi ile güncellemelerin sadece üretici tarafından imzalanan sürümlerinin yapılması sağlanmaktadır. Bu nedenle bu güvenlik hedefi, T.KÖTÜCÜL_GÜNCELLEME tehdidine karşı önlem sağlar.

4.4.3. Çalışma Ortamı için Güvenlik Hedeflerinin Gerekçesi

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_GÜVENLİK varsayımını karşılar.
OE. GÜVENİLİR_YÖNETİCİ	Bu çalışma ortamı güvenlik hedefi, TOE çalışma ortamı üzerinde yönetim yetkisine sahip tüm kullanıcıların gerekli güvenlik denetimlerinden geçmelerini ve güvenlik eğitimin almış tecrübeli kişilerden seçilmelerini sağlar. Bu nedenle, A.GÜVENİLİR_YÖNETİCİ varsayımını karşılar.
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 BT 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_GÜVENLİK varsayımını karşılar.
OE. ZAMAN DAMGASI	Bu çalışma ortamı güvenlik hedefi, güvenlikle ilgili olay kayıtlarının zamanlarının yeterince hassas olarak kaydedilmesi ve değiştirildiğinin tespit edilmesi için zaman damgalarının oluşturmasını sağlar. Bu nedenle, T.GÜNLÜK_BOZMA ve T.VERİ_DEĞİŞTİRME tehditlerine karşı da önlem sağlar.
OE. GÜVENLİ_İLETİŞİM	Bu çalışma ortamı güvenlik hedefi, TOE çalışma ortamındaki iletim ağının güvenilir bir iletişim ortamı sağlamasına olanak verir. Bu nedenle, A.GÜVENLİ_İLETİŞİM varsayımını sağlar. Bunun yanında iletişim ortamının güvenli olması, dağıtık hizmet aksatma saldırısını da etkisiz kılacaktır. Bu nedenle bu güvenlik hedefi, T.HİZMET_AKSATMA tehdidine karşı da önlem sağlar.

5. Genişletilmiş Bileşenler Tanımı

Bu koruma profili, genişletilmiş bir bileşene ihtiyaç duymamaktadır.

6. Güvenlik Gereksinimleri

6.1. Fonksiyonel Güvenlik Gereksinimleri

6.1.1. Genel Bakış

Bu koruma profilinde kapsanan bileşenler, aşağıda tablo-2'de 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_AFL.1	Kimlik doğrulama başarısızlıklarının ele alınması
FIA_SOS.1	Sırların doğrulanması
FIA_UAU.2	Herhangi bir işlemden önce kullanıcı kimlik doğrulama
FIA_UAU.5	Çoklu kimlik doğrulama mekanizmaları
FIA_UID.1	Kimlik tanımlama zamanlaması
FIA_UID.2	Herhangi bir işlemden önce kullanıcı kimlik tanımlama
FIA_USB.1	Kullanıcı-Nesne ilişkilendirme
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 damgaları
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_TRP.1	Güvenilir yol

6.1.2. Fonksiyonel Güvenlik Politikaları

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. Güvenlik Denetimi (FAU)

FAU_GEN.1	**Denetim verilerinin oluşturulması**
Hiyerarşik Bileşen(ler):	Hiyerarşik bileşen yoktur.
Bağımlılıklar:	FPT_STM.1 Güvenilir zaman damgaları

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 kimlik doğrulama 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) 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.KAYIT_TUTMA 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_AFL.1	Başarısız kimlik doğrulama denemelerinde eşik değere ulaşılması ve bu durumda yapılması gereken işlemler, uygulanabilir olması durumunda normal duruma geçiş (terminalin yeniden etkinleştirilmesi gibi)	

FIA_ATD.1	???	
FIA_SOS.1	Test edilmiş herhangi bir sırrın TSF tarafından kabulü ya da reddedilmesi	Tanımlanmış kalite ölçütlerindeki değişikliklerin tanımlanması
FIA_UAU.2	Kimlik doğrulama mekanizmasının başarısız kullanımı; Kimlik doğrulama mekanizmalarının tüm kullanımları	
FIA_UID.1	Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı kimliğini de içeren, başarısız kullanımı, Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı kimliğini de içeren, bütün kullanımı.	Sunulan kullanıcı kimliği, girişimin kaynağı (bağlanan uç tanımlayıcısı, kaynak adres gibi)
FIA_UID.2	Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı kimliğini de içeren, başarısız kullanımı, Kullanıcı tanımlama mekanizmasının, sağlanmış olan kullanıcı kimliğini de içeren, bütün kullanımı.	Sunulan kullanıcı kimliği, 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 kullanıcı 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	Eş zamanlı 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_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.KAYIT_TUTMA 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.

PP 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.KAYIT_TUTMA 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.KAYIT_TUTMA ve O.YETKİLENDİRME hedeflerine katkı sağlar.

FAU_SAR.3 Seçmeli denetimin gözden geçirilmesi

Hiyerarşik Bileşen(ler):	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.

PP 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.KAYIT_TUTMA, 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.KAYIT_TUTMA ve O.BİLGİ_KORUMA 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.KAYIT_TUTMA 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.KAYIT_TUTMA hedefine katkı sağlar.

6.1.4. Kullanıcı Verisinin Korunması (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.

PP 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.BİLGİ_KORUMA 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 oturum 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:** **6) 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.BİLGİ_KORUMA ve O.YETKİLENDİRME hedeflerine katkı sağlar.

6.1.5. Tanıma ve Kimlik Doğrulama (FIA)

FIA_AFL.1 **Kimlik doğrulama başarısızlıklarını işleme**

Hiyerarşik Bileşen(ler):	Hiyerarşik bileşen yoktur.
Bağımlılıklar:	FIA_UAU.1 Kimlik doğrulama zamanlaması
FIA_AFL.1.1	TSF; **[atama: TOE rollerine ait kimlik doğrulama işlemleri]** ile ilgili başarısız kimlik doğrulama girişimlerinin sayısı **[seçim: [atama: pozitif tam sayı]]** sayısına ulaştığını algılamalıdır.
FIA_AFL.1.2	Başarısız kimlik doğrulama girişimlerinin sayısı önceden tanımlanmış sayıya **[seçim: ulaşırsa],** TSF **[atama: TOE fonksiyonlarına erişimin engellemesi]** ni gerçekleştirmelidir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.KİMLİK_DOĞRULAMA hedefine katkı sağlar.

FIA_ATD.1 Kullanıcı öznitelik tanımlama

Hiyerarşik Bileşen(ler):	Hiyerarşik bileşen yoktur.
Bağımlılıklar:	Bağımlılık yoktur.
FIA_ATD.1	TSF **[atama:** **a) Kullanıcı kimlik kodu (uid)** **b) Kullanılan kimlik doğrulama mekanizması** **c) Kullanılan kimlik doğrulama mekanizması için doğrulama bilgileri** **d) Kullanıcı kimlik id si veya T.C. akıllı kimlik kartı için PIN/Parola** **e) T.C. akıllı kimlik kartı numarası** **f) Rol** **]** karşıladığını doğrulayan bir mekanizması olması gerekir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.KİMLİK_DOĞRULAMA hedefine katkı sağlar.

FIA_SOS.1 Sırların doğrulanması

Hiyerarşik Bileşen(ler):	Hiyerarşik bileşen yoktur.
Bağımlılıklar:	Bağımlılık yoktur.
FIA_SOS.1	TSF'nin sırların **[atama:** **a) En az bir büyük harf içermeli** **b) En az bir küçük harf içermeli** **c) En az bir rakam içermeli** **d) En az bir sembol içermeli** **e) En az yedi karakter içermeli** **f) Tekrarlı tahmin edilebilir diziler içermemeli** **]** yukarıdaki şartları karşıladığını doğrulayan bir mekanizması olması gerekir.

Uygulama Notu: Bu SFR kimlik doğrulama mekanizması olarak sadece parola kullanımı için geçerlidir. T.C. Akıllı kimlik kartı için geçerli değildir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.KİMLİK_DOĞRULAMA hedefine katkı sağlar.

FIA_UAU.2	**Herhangi bir işlemden önce kullanıcı kimlik doğrulama**
Hiyerarşik Bileşen(ler):	FIA_UAU.1 Kimlik doğrulamanın zamanlaması
Bağımlılıklar:	FIA_UID.1 Kimlik Tanımlamanın zamanlaması
FIA_UAU.2.1	TSF, herhangi bir kullanıcının yerine TSF tarafından sağlanan eylemleri gerçekleştirmek için kullanıcıya izin vermeden önce, kullanıcının kimliği doğrulamasının başarılı bir şekilde yapılmasını gerektirir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.KİMLİK_DOĞRULAMA hedefine katkı sağlar.

FIA_UAU.5	**Çoklu kimlik doğrulama mekanizmaları**
Hiyerarşik Bileşen(ler):	FIA_UAU.1 Kimlik doğrulamanın zamanlaması
Bağımlılıklar:	FIA_UID.1 Kimlik Tanımlamanın zamanlaması
FIA_UAU.5.1	TSF, kullanıcı kimlik doğrulamasını desteklemek için **[atama:** **a) Kullanıcı kodu ve parola** **b) Token (Akıllı kart dâhil) kimlik doğrulama** **]** Mekanizmalarını sağlayacaktır.
FIA_UAU.5.2	TSF'nin, herhangi bir kullanıcının beyan edilen kimliğini **[atama: yetkili yönetici tarafından belirtilen kimlik doğrulama mekanizması]** kuralına göre doğrulaması gerekir.

Rasyonel: Bu bileşen, FDP_ACC.1 altında tanımlanan erişim kontrol politikasının detay niteliklerini tanımlamaktadır. Bu nedenle aynı şekilde O.KİMLİK_DOĞRULAMA hedefine katkı sağlar.

FIA_UID.1	**Kimlik tanımlama zamanlaması**
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.

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

FIA_UID.2	**Herhangi bir işlemden önce kullanıcı kimlik tanımlama**
Hiyerarşik Bileşen(ler):	FIA_UID.1 Kimlik Tanımlamanın zamanlaması
Bağımlılıklar:	Bağımlılık yoktur.
FIA_UID.2.1	TSF'nin, söz konusu kullanıcının yerine TSF tarafından sağlanan eylemleri gerçekleştirmesine izin vermeden önce her kullanıcının kimliğini tanımlaması gerekir.

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

FIA_USB.1	Kullanıcı-nesne ilişkilendirme
Hiyerarşik Bileşen(ler):	Hiyerarşik bileşen yoktur.
Bağımlılıklar:	FIA_ATD.1 Kullanıcı özniteliği tanımı
FIA_USB.1.1	TSF'nin aşağıdaki kullanıcı güvenlik öznitelikleri ile kullanıcı yerine işlem yapan nesneleri ilişkilendirebilmesi gerekir: **[atama:** **Kullanıcı kimlik kodu (uid)** **Kullanıcı Rolü** **]**
FIA_USB.1.2	TSF'nin kullanıcı güvenlik öznitelikleri ile kullanıcı yerine işlem yapan nesnelerin ilk ilişkilendirebilmesi için aşağıdaki kuralı uygulaması gerekir: **[atama: Başarılı bir kimlik tanımlama ve doğrulama sonrasında kullanıcı adı, başarı ile kimliği doğrulanan kullanıcının kullanıcı adı olacaktır.]**
FIA_USB.1.3	TSF'nin kullanıcının yerine işlem gerçekleştiren nesnelerle ilişkili kullanıcı güvenlik özniteliklerindeki değişiklikleri yöneten aşağıdaki kuralları uygulaması gerekir: **[atama: herhangi bir değişikliğe izin verilmeyecektir.]**

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

6.1.6. Güvenlik Yönetimi (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.KAYIT_TUTMA 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 akışı kontrol 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.KAYIT_TUTMA 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 dâhilinde 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: TSF 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 inkâr tabanlı kararlar için kullanılan özelliklerin yönetimi
FDP_RIP.2	a) Artık bilginin korunmasının ne zaman gerçekleştirileceğinin seçiminin, TOE içerisinden ayarlanabilir olması
FMT_MOF.1	a) TSF 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) TSF 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
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_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

c) Denetçi

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 ve O. YETKİLENDİRME güvenlik hedefinin karşılanmasını amaçlamaktadır.

6.1.7. TSF'nin korunması (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 damgaları**
Hiyerarşiktir:	Başka hiçbir bileşen yoktur.
Bağımlılıklar:	Bağımlılık yoktur.
FPT_STM.1.1 :	TSF'nin kendi kullanımı için güvenilir zaman damgaları sağlayabilmesi gerekir.

Rasyonel: TOE içerisindeki yönetim ve denetim fonksiyonları için güvenilir bir zaman damgası fonksiyonu sağlar. Bu bileşen O.KAYIT_TUTMA, OE.ZAMAN_DAMGASI güvenlik hedeflerinin karşılanmasını amaçlamaktadır.

6.1.8. Hata toleransı (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 güvence 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 erişimi (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 kısıtlanmasını 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 tarihçesi**
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. Güvenilir yollar/kanallar (FTP)

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 güvence 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. Güvenlik Güvence Gereksinimleri

Bu Koruma Profili, OK Bölüm 3 altında yer verilen ve EAL 2 seviyesi için geçerli olan tüm Güvenlik Güvence 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: Güvenlik Güvence Gereksinimleri Bileşen Listesi

Güvence Sınıfı	Güvence Bileşeni İsmi	Bileşen
ADV: Geliştirme	Güvenlik mimarisi tanımlaması	ADV_ARC.1
	Güvenliği zorlayan fonksiyonel belirtim	ADV_FSP.2
	Temel tasarım	ADV_TDS.1
AGD: Kılavuz dokümanlar	Operasyonel kullanıcı kılavuzu	AGD_OPE.1
	Hazırlık prosedürleri	AGD_PRE.1
ALC: Yaşam döngüsü desteği	Merkezi Yönetim (CM) sisteminin kullanımı	ALC_CMC.2
	TOE'nin Merkezi Yönetim bileşeninin parçaları	ALC_CMS.2
	Dağıtım prosedürleri	ALC_DEL.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
	TOE özet özellikleri	ASE_TSS.1
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. Güvenlik Gereksinimleri Gerekçesi

6.3.1. Fonksiyonel Güvenlik Gereksinimleri Bağımlılıkları

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 damgaları	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 TSF 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_AFL.1	FIA_UAU.1 Kimlik doğrulama zamanlaması	FIA_UAU.1
FIA_ATD.1	-	-
FIA_SOS.1	-	
FIA_UAU.2	FIA_UID.1 Kimlik tanımlama zamanlaması	FIA_UID.1
FIA_UAU.5	-	FIA_UID.1
FIA_UID.1	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 Kullanıcı özniteliği tanımı	FIA_ATD.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
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_TRP.1	-	-

6.3.2. Güvenlik Güvence Gereksinimleri Bağımlılıkları

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

Tablo 7: Güvenlik Güvence 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	-	
ASE_CCL.1	ASE_INT.1 ST tanıtımı ASE_ECD.1 Genişletilmiş bileşenlerin tanımı	ASE_INT.1 ASE_ECD.1

	ASE_REQ.1 Beyan edilen güvenlik gerekleri	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. Fonksiyonel Güvenlik Gereksinimleri Kapsamı

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 Seçimi Gerekçesi

EAL seviyesi seçiminde, ürün grubunun gerektirdiği güvenlik gereksinimleri seviyesi dikkate alınmıştır. Ticari ürünler için tercih edilen EAL seviyesi, çoğunlukla EAL2, EAL3 ve EAL4 olmaktadır. EAL5 ve üstü ise akıllı kartlar gibi donanım 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.KAYIT_TUTMA	O.KİMLİK_DOĞRULAMA	O.YETKİLENDİRME	O.BİLGİ_AKIŞI_KNTRL	O.YÖNETİM	O.BİLGİ_KORUMA	O.MAHREMİYET	O.HATA_YÖNETİMİ	O.GÜNCELLEME
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						✓			
	FIA_AFL.1	✓	✓							
	FIA_SOS.1		✓							
	FIA_ATD.1			✓						
	FIA_UAU.2		✓							
	FIA_UAU.5		✓							
	FIA_UID.1		✓	✓						
	FIA_UID.2		✓	✓						
	FIA_USB.1	✓	✓	✓						
	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_TRP.1			✓						✓

Kaynaklar

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

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