WEB SERVİS GÜVENLİĞİ İÇİN

ORTAK KRİTERLER

KORUMA PROFİLİ

Versiyon 1.0

TÜRK STANDARDLARI ENSTİTÜSÜ

İÇERİK

1. PP GİRİŞ

Bu koruma profili (Protection Profile) aşağıdaki öğeleri tanımlar.

- Değerlendirme Hedefi (TOE) ve ilişkili bileşenler,
- Kritik güvenlik ve fonksiyonel özellikler,
- TOE Tipleri,
- TOE Uyumluluk Bildirimini,
- Güvenlik problemi tanımı, bu alan TOE kapsamında tanımlanmıştır. (Varlıklar, Roller, Tehditler ve Varsayımlar)
- Güvenlik Nesneleri,
- Harici Bileşen Tanımı,
- Güvenlik fonksiyonları ve Gereksinimlerin Kapsamında yapılan (Select, Assign, Refinement and Iteration) işlemlerini ve Güvenlik Nesneleri arasındaki ilişkileri,
- PP kapsamında yapılan kısaltmaları,
- PP kapsamında kullanılan Kaynaklar ve Referanslar

1.1 PP Referans

PP Başlığı	**:** Web Servis Güvenliği
Sponsor	**:TÜRK STANDARDLARI ENSTİTÜSÜ**
Editor(ler)	**:TÜRK STANDARTLARI ENSTİTÜSÜ**
CC Versiyon	**:** Version 3.1 Revision 4
Değerlendirme Seviyesi	**:** EAL Level 2
Versiyon Sayısı	**:** 1.0
Anahtar Kelimeler	**:** Web Servis, Güvenlik, Web Servis Fonksiyonları, Denetim

Notlar: PP kapsamında geçen kısaltmalar ile ilgili açıklamaları Kısaltmalar ve Kaynaklar kısmında bulabilirsiniz. (Bölüm 7 ve Bölüm 8)

1.2 TOE Genel Bakış

Bilindiği gibi günümüzde web servisleri uygulamalar arasında verinin paylaşımında oldukça yaygın bir şekilde kullanılmaktadır. Bu kullanım özellikle kurumlar arası veri paylaşımının sağlanması ve veri adacıklarının önlenmesi açısından oldukça önemlidir. Kamu ve Özel kurumlar, sunmuş oldukları hizmetleri günümüz modern Internet çağında e-hizmet haline dönüştürmeye çalışılmaktadır. Bu kapsamda web servisler son derece önemli bir hale gelmektedir. Kurumların sunacakları servislerin sunumu ve diğer elektronik uygulamaların bu hizmetlerden faydalanması son derece önemlidir. Ayrıca birden fazla kurumun sunmuş olduğu web servisleri kullanarak başka kurumlar sunmuş oldukları hizmetlerin kalitelerini ve katma değerlerini arttırmaktadır.

Web servisler ayrıca uygulamaların entegrasyon açısında ciddi kazanımlar sağlamaktadır. Özet olarak aşağıdaki faydaları sayabiliriz.

- **Yazılım Dili Bağımsızlığı:** Geliştirilen ortak standart sayesinde herhangi bir yazılım dilinde (C, Java, PHP v.b.) web servis geliştirilebilmektedir. Bu sayede uygulama geliştirme hızı ve bunu hizmet haline getirilmesi arttırılmaktadır.
- **Platform Bağımsızlığı:** Web servisler farklı platformlarda çapraz bir şekilde çalışabilmektedir. Bu anlamda Web Servisin geliştirildiği dil, framework, kullanılan işletim sistemi, kullanılan veri tabanı sistemi farklı olabilmekte ve en önemlisi web servisi hizmeti sunan uygulama ile bu hizmeti kullanacak olan uygulama farklı yapılarda çalışabilmektedir. (Örneğin, C# ile Microsoft İşletim Sistemlerinde çalışan ve MSSQL veri tabanını kullanarak geliştirilen bir web servis, PHP ile yazılan ve Linux üzerinde çalışan ve MySQL veri tabanı kullanılarak geliştirilen bir uygulama tarafından kullanılabilmektedir.)
- **Kolay Entegrasyon:** Bir uygulama ile başka bir uygulamanın entegrasyonu Web servisler tarafından kolay bir şekilde sağlanabilmektedir.
- **Erişim Kolaylığı:** Web servisleri http protokolü üzerinden çalıştığı için erişimi kolaydır.

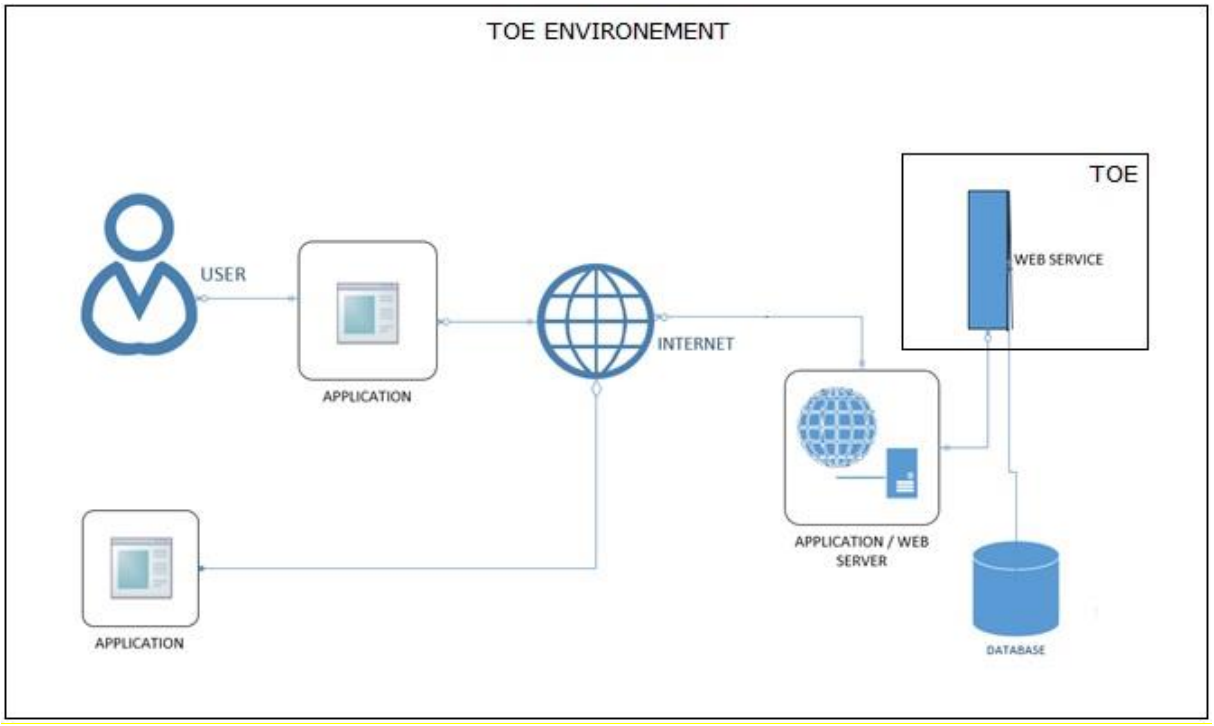
Bu faydaları ile birlikte Web servisler günümüzde farklı tehditlerle karşı karşıya kalmaktadır. Bu nedenle kurumların kullanmış oldukları web servislere yönelik olarak bu koruma profili geliştirilmiştir.

Bu TOE Web servislerine yönelik olarak hazırlanan koruma profilini adresler.

1.2.1 TOE ve Bileşenlerine Genel Bakış

TOE ile ilgili olarak genel yapı Şekil 1 de açıklanmaya çalışılmıştır.

Şekil üzerinden görüldüğü üzere, Kullanıcı herhangi bir tarayıcı uygulamasını kullanarak veya herhangi bir uygulama kendisi Intranet/Internet üzerinden Uygulama/Web Sunucu üzerinden barınan Web Servis uygulamasına erişir. Web Servis uygulaması kendisinde gelen isteği değerlendirerek gerekirse veri tabanı ve diğer alanları kullanarak erişim isteğine cevap verir.



-Şekil 1-

1.2.2 TOE Olmayan Donanım/Yazılım Gerekli Bileşenleri

TOE içerisinde olmayan gerekli Donanım ve Yazılımları aşağıda tanımlanmıştır.

1.2.2.1 TOE Yazılım Ortamı

TOE aşağıda belirtilen yazılım bileşenlerini kullanılır.

İşletim Sistemi: TOE işletim sistemi üzerinde çalışır. Web servisleri ayrıca herhangi bir işletim sistemi üzerinde çalışabilirler. Bu platform bağımsızlığının da bir göstergesidir. (Linux, Microsoft Windows, v.b.).

Uygulama Sunucusu / Web Sunucusu: TOE web servisin çalışması için gereken istekler ve bunlara verilecek cevaplar için herhangi bir uygulama ve web sunucu yazılımı üzerinde çalışabilirler. (IIS, Apache, WebSephire, v.b).

Veri Tabanı Sunucusu: Gelen isteğe göre, TOE veri tabanı ile etkileşimde bulunarak sorgular oluşturabilir ve bunu veri tabanına gönderebilir. Web servisler herhangi bir Veritabanı Sunucusu ile çalışabilir. (Oracle, MSSQL, MySQL, Sysbase, v.b.).

1.2.2.2 TOE Donanım Ortamı

TOE aşağıdaki donanım bileşenleri kullanabilir.

TOE' nin Platform Bağımsız yapısından dolayı Web servis seçilen platforma göre herhangi bir donanım konfigürasyonunda çalışabilir.

1.2.3 Majör Güvenlik ve Fonksiyonel Özellikler

Kritik Güvenlik ve Fonksiyonel Özellikler aşağıda belirtilmiştir.

1.2.3.1 TOE Fonksiyonel Özellikler

TOE fonksiyonel özellikleri aşağıda sıralanmıştır.

- TOE kendisine gelen isteklere cevap verebilmek için sürekli aktif durumda olmalıdır.
- TOE' ye yapılan istekler sürekli olarak filtreden geçirilmelidir. (IP, Zaman v.b.) Filtreye uygun olmayan isteklere reddedilmelidir.
- TOE gelen istekleri kontrol etmelidir. (Şematik, içerik, Parametre, Veri Tipi) İçeriği uygun olmayan istekler reddedilmelidir.
- TOE isteğe vermiş olduğu yanıtlar sırasında gereksiz detayda yanıt vermemelidir. (Hata mesajlarının basitleştirilmesi ve uygun bir şekilde kodlanması).
- TOE belirlenen istek mesaj kapasitesine göre kontrol edilmeli ve kapasite üstü mesajlar reddedilmelidir.
- TOE gelen isteklerin içeriğini virüse yönelik olarak kontrol etmelidir. Bu nedenle TOE tarafından gerekli güvenlik önlemleri alınmalıdır.
- TOE' ye gelen İstekler ve TOE tarafından verilen Cevaplar XML formatına uygun olmalıdır.

1.2.3.2 TOE Güvenlik Özellikleri

TOE ile ilgili olarak olması gereken güvenlik özellikleri şunlardır.

- TOE ile bağlantı güvenli bir şekilde kurulmalıdır.
- TOE kapsamında yapılacak işlemlerde doğrulama mekanizması sağlanmalıdır.
- TOE kapsamında yapılacak işlemlerde yetkilendirme mekanizması sağlanmalıdır.
- TOE kendisine gelen isteklerin mesaj bütünlüğünü sağlamalıdır.
- TOE kendisine yapılan istekleri kayıt altına almalıdır.

1.2.4 TOE Tipi

TOE' nin tipi "Web Servis" 'tir.

1.3 Doküman Yazımı

Bu koruma profilinde kullanılan doküman yazımı ve formatı Ortak Kriterler Versiyon 3.1 Revizyon 4'e uygun olarak yapılmıştır. Seçilen bölümler Koruma Profili okuyucularının daha rahat okumalarına yardımcı olmak için seçilmiştir. Ortak Kriterler bazı fonksiyonel gereksinimler için çeşitli işlemlerin yapılmasına izin verir: Seçilmesine izin verilen işlemler Ortak Kriterler 2. Bölümde tanımlanmıştır.

- Seçme işlemleri bileşenler üzerinde birden fazla öğeyi içeren bir listeden ilgili bir veya birden fazla öğeyi seçme işlemidir. Seçme işlemleri *[sağa yatık /italic metin ile gösterilmiştir*.
- Atama işlemleri bileşenlerüzerinde daha önce belirlenmemiş bir parametre için değer atama işlemidir. Atama işlemleri [Mavi renkli metin] ile gösterilmiştir.

2. UYUMLULUK BİLDİRİMİ

2.1 CC Uyumluluk Bildirimi

Bu koruma profili aşağıdaki dokümanlara uyumlu olduğunu bildirir:

- Ortak Kriterler İçin Bilgi Teknolojileri Güvenlik Değerlendirmesi, Bölüm 1: Bilgilendirme ve Genel Model; Versiyon 3.1, Revizyon 4, Eylül 2012
- Ortak Kriterler İçin Bilgi Teknolojileri Güvenlik Değerlendirmesi, Bölüm 2: Güvenlik Fonksiyonel Bileşenleri; Versiyon 3.1, Revizyon 4, Eylül 2012
- Ortak Kriterler İçin Bilgi Teknolojileri Güvenlik Değerlendirmesi, Bölüm 3: Güvenlik Güvence Gereksinimleri; Versiyon 3.1, Revizyon 4, Eylül 2012
- Ortak Kriterler İçin Bilgi Teknolojileri Güvenlik Değerlendirmesi, Değerlendirme Metodolojisi; Versiyon 3.1, Revizyon 4, Eylül 2012

2.2 PP Bildirimi

Bu PP başka herhangi bir koruma profili ile uyumluluğu içermez.

2.3 Paket Bildirim

Bu PP aşağıdaki güvenlik gereksinimleri ile ilgili paketle uyumludur:

- CC bölüm 3 EAL2 güvence paketi ile uyumludur.

2.4 Uygunluk Bildirim İlişkisi

Bu koruma profili herhangi bir koruma profili ile uygunluk ilişkisi bulunmamaktadır, bu konu uygulanmamıştır.

2.5 Uygunluk Bildirimi

Herhangi bir ST (Güvenlik Hedefi) veya PP(Koruma Profili) bu koruma profiline uygunluk bildiriminde bulunabilir.

3. GÜVENLİK PROBLEM TANIMI

3.1 Giriş

3.1.1 Roller

Web Servis İstemci Kullanıcısı: Kurum tarafından yayınlanan web servise ulaşmak için yetkilendirilmiş kişidir.

Web Servis İstemci Uygulaması: Kurum tarafından yayınlanan web servise ulaşmak için yetkilendirilmiş uygulamadır.

Attak Yapan Kişi (Kötü Niyetli Kişi): Web servis ve fonksiyonlarına illegal yollara erişmek isteyen kişidir. Attak yapan kişi web servise erişmek için yeterli izni olmadığı için böyle bir yönteme başvurur. Atak yapan kişi aynı zamanda web servis tarafından sunulan verilerin kanun dışı yollarla elde edilmesi ve web servisin fonksiyonalitesi ve erişebilirliğini bloklamak isteyebilir.

Sistem Yöneticisi: Web servisin konfigürasyonunu yapan ve güvenliğini sağlayan kişidir. Sistem Yöneticisi, Web servisin hizmet vermesi için gerekli olan tüm donanım ve yazılım bileşenlerinin konfigürasyonunu sağlar.

Tasarımcı: Yayınlanan web servisi ve web servis içerisindeki fonksiyonları tasarlayan kişidir.

Geliştirici: Yayınlanan web servisi ve web servis içerisindeki fonksiyonları geliştiren kişidir.

3.1.2 Varlıklar

Kurumsal Bilgi

Kurum tarafından oluşturulan ve sadece yetkilendirilmiş kullanıcıların erişimine açılan bilgi.

Kurumsal Hizmet

Kurum tarafından paydaşlarına sunulan hizmetler.

XML Mesaj

Web servis tarafından gönderilen veya alınan XML formatındaki bilgi.

3.2 Tehditler

Bu bölüm TOE üzerinde oluşabilecek tehditleri açıklamaktadır. Bu çerçevede TOE tarafından korunan veya kullanılan varlıklarla oluşabilecek tehditler arasındaki ilişki açıklanmıştır.

T.ACCESS CONTROL - T.ACCSCON: Yetkisiz kullanıcı veya uygulama tarafından web servise ve/veya fonksiyona erişilmesi.

Tehdit: Yetkisiz erişim sonucu kurumsal bilginin açığa çıkması

Varlık: Kurumsal Bilgi

T.AUTHORITY DEFINITION - T.DEFIN: Kullanıcının yetkisi dışında web servise ve/veya fonksiyona erişmesi.

Tehdit: Olmayan yetkiyle erişim sonucu kurumsal bilginin açığa çıkması

Varlık: Kurumsal Bilgi

T.DATA MANIPULATION - T.DATAMANIP: Web servislerin kullanılması sırasında XML mesaj içeriğinin değiştirilmesi.

Tehdit: Kötü niyetli kişiler tarafından mesaj içeriğinin değiştirilerek web servisi sunumuna veya içerik değişimden kaynaklı farklı verilere ulaşılması

Varlık: Kurumsal Bilgi, XML Mesajı

T.BLOCK THE ACCESS - T.BLOCKACC: Web servislerine yapılacak hizmet durdurmasına yönelik ataklarla web servislerine yetkili kullanıcı ve/veya uygulamalar tarafından yapılacak erişimin engellenmesi.

Tehdit: Kurum tarafından sunulan hizmetlerin engellenmesi

Varlık: Kurumsal Hizmet

T.WRONG USAGE AND CONFIGURATION - T.WRONGUSANDCONFIG: Yetkisiz ve eğitimsiz personel tarafından yanlış kullanım ve yanlış yapılan konfigürasyon sonrasında web servis hizmetlerinin verilememesi, yetkilendirme sisteminin etkisiz kalması.

Tehdit: Web servis hizmetinin sunulamaması, yetkisiz kişiler tarafından yapılacak erişim

Varlık: Kurumsal Hizmet, Kurumsal Bilgi

T.LOSS OF DATA - T.DATALOSS: Kötü niyetli kişi tarafından kurumsal bilginin hasara uğratılması/ silinmesi durumunda kurumsal hizmetin verilemeyecek hale gelmesi

Tehdit: Kurumsal bilginin hasar görmesi/yok olması, Kurumsal Hizmetin durması

Varlık: Kurumsal Hizmet, Kurumsal Bilgi

T.RECORDS - T.RECORDS: Kayıtların olmaması veya düzgün bir şekilde incelenmemesinden dolayı kötü niyetli kişilerin fark edilmeden web servislerine ve fonksiyonlarına erişmesi

Tehdit: Kurumsal Bilginin açığa çıkması

Varlık: Kurumsal Bilgi

3.3 OSP

Bu bölüm uygulanması gereken kurumsal güvenlik politikalarını tanımlar.

P.SECURITY - P.SECURE: TOE kapsamında çalışacak olan web servislere erişimin sadece yetkilendirilmiş kaynaklar tarafından yapılması sağlanmalıdır. Bu kapsamda gerekli her türlü bileşen kullanılarak (Switch, Router, Firewall, v.b.) gerekli ayarlar (güvenlik kuralları, güvenlik konfigürasyonları) yapılmalı ve her türlü fiziksel ve mantıksal güvenlik önlemleri alınmalıdır.

P.SECURE COMMUNICATION - P.SECCOMM: Sunulan web servisleri ile yapılacak olan iletişim güvenli bir şekilde sağlanmalıdır. Bu kapsamda yapılacak iletişim SSL/TLS protokolleri üzerinden gerçekleştirilmelidir. Web servis sağlayıcısı iletişimi zamanı dolmamış, iptal edilmemiş ve yürürlükten kaldırılmamış sunucu sertifikaları ile sağlamalıdır. Web servis kullanıcısı da her bir kullanım sırasında Web servis sağlayıcısı tarafından sağlanan sertifikayı doğrulamalı ve ondan sonra web servis isteğinde bulunmalıdır. Web servis iletişimi güvenli iletişim protokolü kullanılarak sağlanmalıdır.

P.FILTERING - P.FILTER: Web servise iletişim kapsamında çeşitli filtreler uygulanmalıdır. Bu filtreler aynı anda veya birbirinin yerine kullanılabilir. İki tip filtreleme kullanılabilir. Zaman Filtresi, IP Filtresi.

- Zaman filtresi, sunulan web servise ve/veya fonksiyonuna sadece o fonksiyon tarafından belirlenen zaman dilimlerinde erişimi sağlamalıdır.
- IP filtresi, sunulan web servise sadece belirlenen IP adres bloklarından erişimi sağlamalıdır.

P.SCHEMA VALIDATION - P.SCHEMAVALID: Web servisi kapsamında kullanılan mesajların belirlenen XML şemasına uygun olduğu denetlenmelidir. Schema validasyonundan geçemeyen istekler kabul edilmemelidir.

P.VALIDATION AND AUTHENTICATION - P.VALIDANDAUTH: Web servislere erişim ve ilgili fonksiyonların kullanımı daha önceden tanımlanmış Doğrulama ve Yetkilendirme mekanizması tarafından kontrol edilmeli ve yetkisiz erişimler engellenmelidir.

P.ACCESSIBILITY - P.ACCESSIBILITY: Web servislerinin yoğun kullanımı durumunda hizmetin erişilebilirliğinin sağlanması amacıyla gerekli alt yapı kurulu olmalıdır. Gelen istekler uygun bir şekilde yükü dengelenmeli ve web servislerine erişim sürekli olarak sağlanmalıdır.

P.MESSAGE CAPACITY - P.MESSAGECAP: Web servisleri kapsamında giden ve gelen XML mesajların büyüklüğü için bir mesaj kapasitesi genel olarak veya kullanılan web servis fonksiyonları bazında belirlenmelidir. Gelen web servis istekleri eğer mesaj kapasitesini aşıyorsa reddedilmeli, gönderilecek mesajlar kapasite aşımını önleyecek şekilde gönderilmelidir. (Paging, Dosya aktırımı için farklı erişim yöntemlerinin kullanılması (FTP) v.b.)

P.SCANNER MECHANISM - P.SCANNER: Web servisleri kapsamında giden, gelen mesajlar herhangi bir zararlı yazılım ve kötü niyetli kod parçacığına karşı taranmalı ve zararlı içerik taşıyan istekler reddedilmelidir.

P.LOG RECORDS - P.RECLOG: Web servislerine yapılan her türlü erişim (Erişim yapan IP, Zaman, Erişim yapılan fonksiyon, Erişimi Gerçekleştiren kullanıcı) gibi bilgilerle kayıt altına alınmalıdır.

P.MAINTENANCE - P.MAINTENANCE: Web servisleri sürekli olarak kontrol edilmeli ve değişen teknoloji ve ihtiyaçlara göre gerekli güvenlik güncellemeleri yapılmalıdır. Ayrıca alınan kayıtlar (P.LOG) incelenmeli ve varsa yetkisiz erişimler tespit edilerek gerekli güvenlik önlemleri arttırılmalıdır. Ayrıca her yeni eklenen web servis ve fonksiyonun gerekli yetkilendirmeleri kontrol edilmeli her yeni eklenen kullanıcının tanımları kontrol edilmelidir. Benzer şekilde iptal edilen fonksiyonlar ve iptal edilen kullanıcılara göre güvenlik önlemleri güncellenmelidir.

3.4 Varsayımlar

Bu bölüm TOE kapsamında belirlenen varsayımları tanımlar.

A.DESIGNER SECURITY - A.DESIGNERSEC: TOE kapsamında çalışacak olan Web servislerin yapısı güvenlilir tasarımcı tarafından yapılır. Güvenilir tasarımcılar herhangi bir şekilde güvenlik riski ortaya çıkartacak şekilde veya herhangi bir dizayn açığı (arka kapı v.b.) bırakacak şekilde yapıyı tasarlamazlar. Güvenilir Tasarımcıların TOE kapsamında geliştirilecek Web servislerinin mümkün olan en iyi şekilde güvenlik özelliklerini karşılayacak şekilde Web servisleri tasarladıkları varsayılır.

A.DEVELOPER SECURTIY - A.DEVELOPERSEC: Güvenilir programcılar tarafından geliştirilen web servislerinin, herhangi bir arka kapı ve güvenliği ihlal edecek herhangi bir kod parçası içermediği varsayılır. Güvenilir programcıların TOE kapsamında geliştirilecek Web servislerinin mümkün olan en iyi şekilde güvenlik özelliklerine uygun şekilde Web servislerini programladıkları varsayılır.

A.ENVIRONMENT SECURITY - A.ENVSEC: TOE' nin çalışacağı İşletim Sistemi, Veri Tabanı, Uygulama Sunucu, Web sunucusu ve diğer bileşenlerin en son güvenlik ayarlarının yapıldığı, bütün güvenlik açıklarının kapatıldığı ve tüm olası tehditlere karşı gerekli güvenlik önlemlerinin alındığı varsayılır.

A.PHYSICAL PROTECTION - A.PHYSICALPROTECT: TOE' nin çalışacağı ortamın ve yazılım ve donanım bileşenlerinin fiziksel olarak koruma altında olduğu ve yetkisiz kişiler tarafından erişimi önlemek için gerekli fiziksel güvenlik önlemlerinin alındığı ve erişime kapalı olduğu varsayılır.

A.PERSONEL TRAINING - A.TRAINEDPERS: TOE kapsamında çalışacak olan yazılım ve donanımsal bileşenlerin yapılandırılması, konfigüre edilmesi, çalıştırılması ve korunmasına yönelik alınacak olan aksiyonların yetkili ve konuyla ilgili olarak gerekli eğitimi almış yetkili personel tarafından yapıldığı varsayılır.

4. SECURITY OBJECTIVES

4.1 TOE' nin Güvenlik Nesneleri

Bu bölüm TOE tarafından sağlanan güvenlik nesnelerini tanımlar.

O.ACCESS CONTROL - O.ACCONTROL: TOE web servislerine ve fonksiyonlarına yönelik erişimi kontrol etmelidir.

O.VALIDATION AND AUTHENTICATION - O. VALAUTH: TOE doğrulama ve yetkilendirme mekanizmasını çalıştırmalıdır.

O.INTEGRITY - O.INTEGRITY: TOE kullanılan XML mesajlarının bütünlüğünü sağlamalıdır.

O.RECORDS - O.RECORDS: TOE yapılan tüm erişimleri kayıt altına almalıdır.

O.AUTHORIZE - O.AUTHORIZE: TOE kapsamında yapılacak her türlü yazılım ve donanım bileşenlerinin fiziksel ve mantıksal yapılandırılması ve konfigürasyonu yetkili kişi tarafından yapılmalıdır.

4.2 Operasyonel Ortamın Güvenlik Nesneleri

Bu bölüm TOE tarafından sağlanan çalışma ortamına yönelik güvenlik nesnelerini tanımlar.

OE.PHYSICAL PROTECTION - OE. PHYSPRTC: TOE fiziksel olarak korunmuş ve sadece yetkili personel tarafından erişilebilir bir ortamda bulunmalıdır.

OE.PERSONEL TRUST - OE. TRUSTPER: TOE sadece güvenilir personel tarafından dizayn edilmeli, geliştirilmeli, güncellenmeli, yapılandırılmalı ve konfigüre edilerek hizmet vermeli ve hizmetin sürekliliği sağlanmalıdır.

OE.TRAINING - OE. TRAINING: TOE kapsamında kullanılacak olan güvenilir personele gerekli eğitim verilmelidir.

OE.ENVIRONMENT SECURITY - OE. SECENV: TOE' nin yetkisiz olarak erişilmesi, var olan yetkinin dışında kullanılması, hizmetin durdurulmaya çalışılmasını engelleyecek her türlü fiziksel ve mantıksal bileşenle koruma altına alınmalı ve gerekli konfigürasyon yetkili personel tarafından sağlanarak güvenilir ortam sağlanmalıdır.

OE.DEVELOPMENT - OE. DEVLP: Tasarımcı ve Geliştiriciler geliştirmiş oldukları yazılımın bilgi güvenliği ile ilgili olarak gerekli kontrolleri sağladığı ve herhangi bir güvenlik açığı oluşturmayacağına emin olmalıdırlar.

4.3 Güvenlik Nesnelerinin İlişkisi

4.3.1 TOE Güvenlik Tehditlerinin İlişkisi

TEHDİT	İLİŞKİ
T.ACCSCON	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erişimin kontrol altına alındığına emin olur.
T.DEFIN	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur.
T.DATAMANIP	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır.
T.BLOCKACC	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur. •

T.WRONGUSANDCONFIG	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.RECORDS TOE' ye yapılan tüm erişimlerin kayıt altına alındığından emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur.
T.DATALOSS	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur.
T.RECORDS	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erişimin kontrol altına alındığına emin olur. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur. • O.RECORDS TOE' ye yapılan tüm erişimlerin kayıt altına alındığında emin olur. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur.

4.3.2 TOE Kurumsal Güvenlik Politikası ile İlişkisi

OSP	İLİŞKİ
P.SECURE	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur. • OE.PHYSPRTC TOE'nin bulunduğu fiziksel ortamın güvenli olduğu ve sadece yetkili personel tarafından erişilebildiğine emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur.

	• OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur.
P.SECCOMM	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır. • OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur.
P.FILTER	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur.
P.SCHEMAVALID	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır.
P.VALIDANDAUTH	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur.
P.ACCESSABILITY	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur.
P.MESSAGECAP	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır.
P.SCANNER	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.INTEGRITY XML mesajlarının bütünlük gereksinimleri TOE tarafından sağlanır.
P.RECLOG	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur. • O.RECORDS TOE tarafından bütün erişimlerin kayıt altına alındığından emin olur.

	• OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur.
P.MAINTENANCE	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.ACCCONTROL TOE tarafından web servis ve fonksiyonlarına yapılan erşimin kontrol altına alındığına emin olur. • O.VALAUTH TOE tarafından doğrulama ve yetkilendirme mekanizmasının çalıştırıldığından emin olur. • O.RECORDS TOE tarafından bütün erişimlerin kayıt altına alındığından emin olur. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur.

4.3.3 TOE Varsayımlarla İlişki

VARSAYIMLAR	İLİŞKİ
A.DESIGNERSEC	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur. • OE.DEVLP TOE'nin dizayn edilmesi ve geliştirilmesi sırasında Geliştirici ve Tasarımcı tarafından yapılan faaliyetler kapsamında herhangi bir açıklığa meydan verecek geliştirme faaliyetinin yapılmadığı ve açıklıkların önlenmesi için gerekli güvenlik önlemlerinin alındığına emin olur.
A.DEVELOPERSEC	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur.

	• OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur. • OE.DEVLP TOE'nin dizayn edilmesi ve geliştirilmesi sırasında Geliştirici ve Tasarımcı tarafından yapılan faaliyetler kapsamında herhangi bir açıklığa meydan verecek geliştirme faaliyetinin yapılmadığı ve açıklıkların önlenmesi için gerekli güvenlik önlemlerinin alındığına emin olur.
A.ENVSEC	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.PHYSPRTC TOE'nin bulunduğu fiziksel ortamın güvenli olduğu ve sadece yetkili personel tarafından erişilebildiğine emin olur. • OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur.
A.PHYSICALPROTECT	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.PHYSPRTC TOE'nin bulunduğu fiziksel ortamın güvenli olduğu ve sadece yetkili personel tarafından erişilebildiğine emin olur. • OE.SECENV Yetkisiz erişim, servis kesintileri gibi problemlerin önlenebilmesi için gerekli olan konfigürasyonların yetkili ve deneyimli personel tarafından yapıldığı ve TOE'nin güvenilir bir ortamda bulunduğuna emin olur.
A.TRAINEDPERS	Bu tehdit aşağıdaki güvenlik nesneleri ile ilişkilendirilmiştir. • O.AUTHORIZE TOE kapsamındaki tüm donanım ve yazılım bileşenlerine yapılacak her türlü fiziksel ve mantıksal konfigürasyonun yetkilendirilmiş personel tarafından yapıldığına emin olur. • OE.TRUSTPER TOE kapsamında yapılan dizayn, geliştirme, güncelleme ve konfigürasyon işlerinin güvenilir personel tarafından yapıldığına emin olur. • OE.TRAINING TOE kapsamındaki personele gerekli eğitimin verildiğinden emin olur. • OE.DEVLP TOE'nin dizayn edilmesi ve geliştirilmesi sırasında Geliştirici ve Tasarımcı tarafından yapılan faaliyetler kapsamında herhangi bir açıklığa meydan verecek geliştirme faaliyetinin yapılmadığı ve açıklıkların önlenmesi için gerekli güvenlik önlemlerinin alındığına emin olur.

		TEHDİTLER							KURUMSAL GÜVENLİK POLİTİKALARI										VARSAYIMLAR				
		T.ACCSCON	T.DEFIN	T.DATAMANIP	T.BLOCKACC	T.WRONGUSANDCONFIG	T.DATALOSS	T.RECORDS	P.SECURE	P.SECCOMM	P.FILTER	P.SCHEMAVALID	P.VALIDANDAUTH	P.ACCESSABILITY	P.MESSAGECAP	P.SCANNER	P.RECLOG	P.MAINTENANCE	A.DESIGNERSEC	A.DEVELOPERSEC	A.ENVSEC	A.PHYSICALPROTECT	A.TRAINEDPERS
GÜVENLİK NESNELERİ	**O.ACCONTROL**	X						X	X	X	X			X			X	X					
	O.VALAUTH		X					X	X		X		X				X	X					
	O.INTEGRITY			X			X			X		X			X	X							
	O.RECORDS					X		X									X	X					
	O.AUTHORIZE						X	X										X	X	X	X	X	X
OPERASYONEL ORTAM	**OE. PHYSPRTC**								X												X	X	
	OE. TRUSTPER					X		X									X	X	X	X			X
	OE. TRAINING					X		X	X									X	X	X			X
	OE. SECENV				X	X			X	X				X							X	X	
	OE. DEVLP																		X	X			X

5. HARİCİ BİLEŞEN TANIMI

Bu Koruma Profilinde, CC bölüm 2 ve 3 uyumluluğu kapsamında herhangi bir harici bileşen tanımlanmamıştır.

6. GÜVENLİK GEREKSİNİMLERİ

Bu bölüm TOE kapsamında uygulanan Güvenlik Fonksiyon Gereksinimleri (SFR), Güvenlik Güvence Gereksinimlerini (SAR) ve Güvenlik Gereksinim ilişkilerini açıklar.

6.1 TOE için Güvenlik Fonksiyonel Gereksinimleri

SINIF	SINIF AİLESİ	AÇIKLAMA	SEÇ	ATA	GELİŞTİR	YİNELE
Güvenlik Denetimi	FAU_GEN.1	Denetim Verisi Oluşturma	X	X		
	FAU_GEN.2	Kullanıcı Tanımlama İlişkisi				
	FAU_SAR.1	Denetimin Gözden Geçirilmesi		X		
	FAU_SEL.1	Seçilen Denetimler	X	X		
	FAU_STG.1	Denetim Kayıtlarının Güvenli Bir Şekilde Saklanması	X			
İletişim	FCO_NRO.1	Göndericinin Onaylanması	X	X		
	FCO_NRR.1	Alıcının Onaylanması	X	X		
Kullanıcı Verisi Koruma	FDP_ACC.1	Erişim Kontrol Setleri		X		
	FDP_ACF.1	Erişim Kontrol tabanlı güvenlik özellikleri		X		
	FDP_DAU.1	Temel Veri Yetkilendirme		X		
	FDP_IFC.1	Bilgi Akış Kontrol Setleri		X		
	FDP_IFF.1	Temel Güvenlik Özellikleri		X		
Tanımlama ve Yetkilendirme	FIA_AFL.1	Yetkilendirme Hata Yönetimi	X	X		
	FIA_ATD.1	Kullanıcı Özellik Tanımlama		X		
	FIA_SOS.1	Gizlilik Mesajının Kontrol Edilmesi		X		
	FIA_SOS.2	TSF Gizlilik Mesajının Oluşturulması		X		
	FIA_UAU.1	Yetkilendirme		X		
	FIA_UAU.6	Tekrar Yetkilendirme		X		
	FIA_UID.1	Tanımlama		X		

Güvenlik Yönetimi	FMT_MOF.1	Güvenlik Fonksiyon davranışlarının yönetimi	X	X		
	FMT_MSA.1	Güvenlik özelliklerinin yönetimi	X	X		
	FMT_MSA.3		X	X		
	FMT_MTD.1	TSF verisinin yönetimi	X	X		
	FMT_SAE.1	Zaman limitli yetkilendirme		X		
	FMT_SMF.1	Güvenlik Fonksiyonlarının Özellikleri		X		
	FMT_SMR.1	Güvenlik Rolleri		X		
TSF' in Korunması	FPT_STM.1	Erişilebilir Zaman Damgası				
Kaynak Optimizasyonu	FRU_RSA.1	Maksimum Kota	X	X		
Güvenli Yol/ Kanallar	FTP_ITC.1	Dahili-TSF güvenli kanal	X	X		
	FTP_TRP.1	Güvenli Yol	X	X		

6.1.1 Güvenlik Denetim Sınıfı (FAU)

6.1.1.1 FAU_GEN.1 Denetim Verisi Üretimi

Açıklama: Kaydedilecek her bir kayıt ve özellikleri ile birlikte seviyesi belirlenmiş denetim olayları için üretilecek denetim kayıtlarını tanımlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FPT_STM.1 Erişilebilir zaman damgası

FAU_GEN.1.1 TSF aşağıdaki denetim olayları için denetim kayıtları üretecektir:

a) Açma ve Kapama denetim fonksiyonları;

b) Bütün denetim olaylarının seviyesi [*temel*] olarak belirlenmiştir; ve aşağıdaki olaylarda uygulanır.

c) [Kullanıcı Tanımlama ve Yetkilendirme, Web Servis ve Fonksiyonlarına erişim].

FAU_GEN.1.2 Her bir denetim kaydı en az aşağıdaki bilgileri içermelidir.:

a) Olayın Tarih ve Zaman bilgisi, olayın tipi, olayı gerçekleştiren (eğer mümkünse), olayın sonucu (başarılı veya hatalı) ve

b) PP/ST' de tanımlı fonksiyonel bilşenleri baz alan her bir denetim olay tipi [Kullanıcı Adı, Tarih/Zaman, Kaynak IP Adresi ve Web Servis Fonksiyonları].

FAU_GEN.2 Kullanıcı Kimlik İlişkilendirme

Açıklama: Kullanıcı kimlik İlişkilendirme, TSF tarafından her bir denetim olayı ile kullanıcıların ilişkilendirilmesini sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FAU_GEN.1 Denetim verisi üretimi

FIA_UID.1 Tanımlama Zamanı

FAU_GEN.2.1 Tespit edilen kullanıcıların eylemlerinden kaynaklanan denetim olayları için, TSF olaya neden olan kullanıcı kimliği ile her denetlenebilir olayı ilişkilendirebilir.

Her bir PP fonksiyonel bileşeni tarafından tanımlanabilecek olay tipleri örnek olarak aşağıda verilmiştir.

- **a.** TSF tarafından kontrol edilen nesneler,
- **b.** Nesnelerin silinmesi,
- **c.** Güvenlik özelliklerinin özne ve nesne bilgilerinin değiştirilmesi,
- **d.** Tanımlama ve yetkilendirme fonksiyonlarının kullanılması.

SFR	Denetim Olayları	Ayrıntılı Bilgi
FAU_SAR.1	Denetlenebilir olaylardan veri okuma	Erişim, Veri Tabanı, Firewall, Uygulama ve Web Sunucu Kayıtları
FAU_SEL.1	Web servis erişim olayları ve Kullanıcı Tanımlama Bilgileri	Web Servis İstemci Uygulama Kullanıcı Bilgisi
FAU_STG.1	Korumalı Denetim Kayıtları	Yetkisiz bir şekilde denetim kayıtlarının silinmesi ve değiştirilmesi
FDP_ACF.1	SFP erişim kontrol olayları ve güvenlik özellikleri	SFP nesneleri tanımlama bilgileri
FIA_UID.1	TSF aksiyonları hakkında Tanımlama ve Yetkilendirme bilgileri	Kullanıcı tanımlama bilgileri
FMT_MOF.1	Fonksiyon davranışlarını değiştirme, aktif ve pasif etme	Web Hizmeti ve Tanımlama
FMT_MSA.1	Güvenlik özellikleri ve aksiyonlar	Bilgi akış kontrolleri ve tanımlı erişim kontrolleri
FMT_MTD.1	TSF Veri yönetim olayları	
FMT_SMF.1	Yönetim fonksiyon özellikleri	Yönetim fonksiyonlarının listesi

SFR	Denetim Olayları	Ayrıntılı Bilgi
FMT_SMR.1	Güvenlik Rolleri	
FPT_STM.1	Erişilebilir Zaman Damgası	
FTP_ITC.1	Sağlanan Güvenli İletişim Kanalı	
FTP_TRP.1	Sağlanan İletişim Yolu	

6.1.1.2 FAU_SAR.1 Denetim Gözdengeçirme

Açıklama: Denetim gözden geçirme, denetim kayıtlarından oluşan bilgilerin okunabilmesini sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FAU_GEN.1 Denetim verisi üretme

FAU_SAR.1.1 TSF [Sistem Yöneticisi]'nin [erişim kayıtları, veritabanı kayıtları, firewall kayıtları ve uygulama ve web server kayıtları] denetim kayıtlarını okunabilmesini sağlar.

FAU_SAR.1.2 TSF bilgileri yorumlamak için kullanıcı için uygun denetim kayıtları sağlayacaktır.

6.1.1.3 FAU_SEL.1 Seçilen Denetimler

Açıklama: Seçilen denetim PP/ST yetkilisi tarafından belirlenen niteliklere bağlı olarak, tanımlanan FAU_GE1 ve tüm denetim olayları içerisinden olay setini gerekli kılar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FAU_GEN.1 Denetim veri üretimi

FMT_MTD.1 TSF data Yönetimi

FAU_SEL.1.1 TSF aşağıdaki özelliklere dayanarak tüm denetim olayları içerisinde seçim yapabilir.:

a) [Nesne Tanımı, Kullanıcı Tanımı, Host Tanımı ve Olay Tipi]

b) [Web Servis Fonksiyonları, Web Servis İstemci Kullanıcısı, Web Servis İstemci Uygulaması(Host), Web Servis Erişimi, Kullanıcı Tanımlama ve Yetkilendirme]

6.1.1.4 FAU_STG.1 Denetim Kayıtlarının Korunması

Açıklama: Denetim kayıtlarının saklanması ve korunması, yetkisiz bir şekilde kayıtların değiştirilmesi ve silinmesi durumuna karşı verilerin güvenli bir şekilde korunmasını zorunlu kırar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FAU_GEN.1 Denetim verilerinin üretilmesi

FAU_STG.1.1 TSF yetkisiz silinmelere karşı saklanmış denetim kayıtlarını korur.

FAU_STG.1.2 TSF saklanmış denetim kayıtları içerisindeki yapılan yetkisiz değişimleri [*tespit*] eder.

6.1.2 İletişim Sınıfı (FCO)

6.1.2.1 FCO_NRO.1 Seçili Kaynak Doğrulama

Açıklama: Seçili Kaynak Doğrulama, konu ile ilgili gerçek kaynağa doğru bir erişimin yapılabilmesi için TSF' e ihtiyaç duyar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FIA_UID.1 Tanımlama Zamanı

FCO_NRO.1.1 İletilen [Web Servisi Client Kullanıcısı ve Uygulaması] ve talebi oluşturan [*yaratan kişi*] için TSF kökenli kanıt üretmek mümkün olacaktır.

FCO_NRO.1.2 TSF [IP Adresi, Kullanıcı Adı ve Şifre] gibi bilgilerin yaratıcısı ve [Web Servis Fonksiyonları] ile ilgili bilgilerin delil olarak uygulanması mümkün olacaktır.

FCO_NRO.1.3 TSF [*bilginin yaratıcısı*] tarafından seçili [kaynak kanıt limitlerini] bilginin kaynağı olarak gösterebilme yeteneğine sahiptir.

6.1.2.2 FCO_NRR.1 Seçili Kaynak Alınması

Açıklama: Seçili kaynak alınması, temin etmek üzere TSF' ten bilginin alınmasından kanıt istemek için yetenek gerektirir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FIA_UID.1 Tanımlama Zamanı

FCO_NRR.1.1 TSF [*iletiyi gönderen kişi (yaratıcısı)*] tarafından almış olduğu [Web Servis Client Kullanıcısı ve Uygulaması] isteklerini seçili kaynakların alınması için kanıt oluşturacaktır.

FCO_NRR.1.2 TSF kanıt oluşturmak için ilgili [IP Adresi, Kullanıcı adı ve Şifre] bilgilerini ve [Web Servisi Fonksiyonlarının] bilgilerini uygulayabilir.

FCO_NRR.1.3 TSF, [*iletiyi gönderen kişi (yaratıcısı)*] tarafından verilen [kanıtlı kök limit] bilgilerinin alındığı delilleri doğrulamak için bir yetenek sağlar.

6.1.3 Kullanıcı Verisi Koruma Sınıfı (FDP)

6.1.3.1 FDP_ACC.1 Erişim Kontrol Altseti

Açıklama: Erişim kontrol altseti, TOE içerisinde bulunan nesnelere yönelik olarak yapılacak işlemler için tanımlanmış erişim kontrol SFP' sini gerekli kılar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FDP_ACF.1 Erişim Kontrol tabanlı güvenlik özelliği

FDP_ACC.1.1 TSF [Web Servis fonksiyonlarına erişimi] [SFP erişim kontrol] üzerinden yapılmasını zorunlu kılar.

6.1.3.2 FDP_ACF.1 Güvenlik Tabanlı Erişim Kontrolü

Açıklama: Güvenlik özellik tabanlı erişim kontrolü TSF güvenlik nitelikleri ve niteliklerin belirtilen gruplara dayalı erişimi zorlamak için izin verir. Ayrıca, TSF açıkça güvenlik nitelikleriyle dayalı bir nesneye erişim izni ya da reddetmek için yeteneğine sahip olabilir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FDP_ACC.1 Erişim Kontrol Altseti

FMT_MSA.3 Statik Özellikli Başlatma

FDP_ACF.1.1 TSF belirtilen nesnelere [SFP tarafından kontrol edilen nesne ve öznelerin listeleri, ver her birinin SFP ile bağlantılı güvenlik özellikleri ve grupları] [SFP erişim kontrolü] uygulanmasını zorunlu kılar.

FDP_ACF.1.2 TSF kontrollü özneler ve kontrollü nesneler arasında bir operasyon izin olup olmadığını belirlemek için aşağıdaki kuralları uygulamayı zorlar: [kontrollü nesneler üzerinde kontrol işlemleri kullanılarak kontrol özneler ve kontrollü nesneler arasında erişimi düzenleyen kurallar].

FDP_ACF.1.3 TSF aşağıdaki ek kurallara göre nesnelere öznelerin erişimine izin verir: [kurallar, güvenlik özelliklerine dayanan, nesnelere öznelerin erişim yetkisi].

FDP_ACF.1.4 TSF ek kurallara göre öznelerin nesnelere erişimini reddeder. [kurallar, güvenlik özellikleri, öznelerin nesnelere olan erişimin kısıtlanması].

6.1.3.3 FDP_DAU.1 Temel Veri Kimlik Doğrulaması

Açıklama: Temel Veri Kimlik Doğrulaması, TSF nesnelerin bilgi içeriği orijinalliğini garanti üretme yeteneğine sahip olmasını gerektirir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FDP_DAU.1.1 TSF geçerlilik teminatı olarak kullanılabilecek kanıt oluşturmak için [Web Servis Client Kullanıcısı ve Uygulaması] bilgi yeteneği sağlayacaktır.

FDP_DAU.1.2 TSF belirtilen bilgilerin geçerliliğinin kanıtı doğrulamak için [Web Servisine Erişim] yeteneğini sağlayacaktır.

6.1.3.4 FDP_IFC.1 Bilgi Akışı Kontrolü Altseti

Açıklama: Bilgi akışı kontrolü altseti, TOE' nin tespit edilen her bilgi akışı kontrolü SFP bilgilerinin bir alt kümesi üzerinde olası operasyonları için bir yerde olmasını gerektirir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FDP_IFF.1 Basit Güvenlik Nitelikleri

FDP_IFC.1.1 TSF [SFP Bilgi Akış Kontrolünün] [özneler listesi, bilgiler ve kontrollü bilgi akışına sebep olan kontrollü konuları SFP tarafından kapsayan operasyonlar], üzerinden zorlar ve kapsar.

6.1.3.5 FDP_IFF.1 Basit Güvenlik Nitelikleri

Açıklama: Basit güvenlik özelliklerini güvenlik nitelikli bilgiler gerektiren, bilgi ve bu bilginin alıcısı olan konularda bilgi sağlar. Bu fonksiyon tarafından uygulanması gereken kuralları belirler ve güvenlik özellikleri fonksiyonu ile elde edilir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FDP_IFC.1 Bilgi Akışı Kontrolü Altseti

FMT_MSA.3 Statik Nitelikli Başlatma

FDP_IFF.1.1 TSF aşağıdaki güvenlik özellikleri bilgileri ve tiplere göre [SFP bilgi akış kontrolü] uygulanmasını zorunlu kılar:[özneler listesi ve SFP kontrolü altındaki kontrollü bilgiler ve her bir bilginin güvenlik özellikleri].

FDP_IFF.1.2 TSF, aşağıdaki kurallar uyulması durumunda kontrollü bir operasyon yoluyla kontrollü bir özne ve kontrollü bilgi arasında bir bilgi akışını izin verir: [her işlem için, güvenlik özellikleri bilgisi ile özneler arasındaki ilişkiyi güvenlik özellik tabanlı oluşturmak gereklidir.].

FDP_IFF.1.3 TSF [ek SFP bilgi akış kontrol kuralları] zorunlu kılar.

FDP_IFF.1.4 TSF kurallara dayalı [güvenlik özellikleri, izin verilecek bilgi akışları] bir bilgi akışına izin verir.

FDP_IFF.1.5 TSF kurallara dayalı [güvenlik özellikleri, engellenecek bilgi akışları] bir bilgi akışını engeller.

6.1.4 Tanımlama ve Yetkilendirme Sınıfı (FIA)

6.1.4.1 FIA_AFL.1 Kimlik Doğrulama Hatası İşleme

Açıklama: Kimlik doğrulama hatası işleme, TSF başarısız kullanıcı kimlik doğrulama girişimleri belirli bir sayıdan sonra oturumunun kurulması süreci sonlandırmanın mümkün olmasını gerektirir. Ayrıca bir yönetici tanımlı durum oluşuncaya kadar oturumunun kurulması sürecinin sona ermesinden sonra, TSF hangi girişimleri yapmış kullanıcı hesabı veya giriş (örneğin iş istasyonu) noktasını devre dışı bırakmaktadır.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FIA_UAU.1 Kimlik Zamanlaması

FIA_AFL.1.1 TSF [Kullanıcı Tanımlama ve Yetkilendirme] esnasında *konfigüre edilebilen pozitif tamsayılardan* [3-5] defa gerçekleşen başarısız kimlik doğrulama girişimlerini tespit eder.

FIA_AFL.1.2 Başarısız kimlik doğrulama girişimlerini tanımlayan numaralar [*aşıldığı zaman]*, TSF [Kullanıcı Hesabını Pasif ya da Devre Dışı] bırakır.

6.1.4.2 FIA_ATD.1 Kullanıcı Özellik Tanımlama

Açıklama: Kullanıcı özellik tanımlama, kullanıcı güvenlik özelliklerinin her bir kullanıcı için tanımlanmasını ve idame ettirilmesini izin verir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FIA_ATD.1.1 TSF her bir kullanıcı için belirlenen güvenlik özellik listelerinin idame ettirilmesine izin verir: [Kullanıcı adı ve Şifre, Host IP Adresi, Çalışılacak zaman aralığı].

6.1.4.3 FIA_SOS.1 Güvenlik Mesajlarının Doğrulanması

Açıklama: Güvenlik mesajlarının doğrulanması, TSF tarafından belirlenen kalite metriklerine göre güvenlik mesajlarının doğrulanmasını gerekli kılar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FIA_SOS.1.1 TSF belirlenen şartlar çerçevesinde güvenlik mesajlarının doğrulanması mekanizmasını sağlar. [tanımlı kalite metriği (Tanımlı Zaman-aşımı değeri)].

FIA_SOS.2 TSF Güvenlik Mesajlarının Üretilmesi

Açıklama: Güvenlik mesajlarının üretilmesi, TSF tarafından belirlenen kalite metriklerine uygun güvenlik mesajlarının üretilmesin sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FIA_SOS.2.1 TSF belirlenen metrikler çerçevesinde güvenlik mesajlarının üretilmesini sağlar. [tanımlı kalite metriği (Tanımlı Zaman-aşımı değeri)].

FIA_SOS.2.2 TSF [FIA_UAU ve FIA_UID] olayları kapsamında güvenlik mesajlarının üretilmesini zorunlu kılar.

6.1.4.4 FIA_UAU.1 Kimlik Zamanlaması

Açıklama: Kimlik Zamanlaması, kullanıcıya kullanıcının kimlik doğrulamasının önceliklendirilmesi ve belirli eylemleri gerçekleştirmesi için aksiyon almasını sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FIA_UID.1 Tanımlama Zamanlaması

FIA_UAU.1.1 Kullanıcı doğrulama işleminden önce TSF, yapılacak kullanıcı adına [TSF aracılı eylemlerin listesine] izin verir.

FIA_UAU.1.2 TSF, TSF-aracılı eylemleri izin vermeden önce her kullanıcının kimlik doğrulamasını gerekli kılar.

FIA_UAU.6 Tekrar Yetkilendirme

Açıklama: Tekrar Yetkilendirme, kullanıcıların tekrar yetkilendirilmesini gereken özel olayların tanımlanmasını sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FIA_UAU.6.1 TSF kullanıcıları bu şartlar altında tekrar yetkilendirir. [FIA_SOS.2 tarafından üretilen mesajın geçersiz olması durumunda].

6.1.4.5 FIA_UID.1 Tanımlama Zamanlaması

Açıklama: Tanımlama Zamanlaması, kullanıcıya TSF tarafından tanımlanmadan önce belirli eylemleri gerçekleştirmesi için aksiyon almasını sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FIA_UID.1.1 TSF, kullanıcı tanımlanma işleminden önce [TSF-aracılı eylemlerin listesinin] çıkarılmasına izin verir.

FIA_UID.1.2 TSF, her bir kullanıcının başarılı bir şekilde tanımlanmasını diğer TSF-aracılı işlemlerinin kullanıcılar tarafından oluşturulmasından önce gerekli görmektedir.

6.1.5 Güvenlik Yönetimi Sınıfı (FMT)

6.1.5.1 FMT_MOF.1 Güvenlik fonksiyonlarının davranış yönetimi

Açıklama: Güvenlik fonksiyonları davranış yönetimi yetkili kullanıcılar (roller) kurallarını kullanmak veya yönetilebilir olabilir. Belirtilen koşullara sahip TSF fonksiyonların davranışlarını yönetmek için izin verir

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FMT_SMR.1 Güvenlik Rolleri

FMT_SMF.1 Yönetim Fonksiyonlarının Özellikleri

FMT_MOF.1.1 TSF [Sistem Yöneticisi] tarafından [Web Servis Erişim ve Tanımlama] fonksiyon [*davranışlarının aktif etme, pasif etme ve değiştirme*] yeteneğini kısıtlamak zorundadır.

6.1.5.2 FMT_MSA.1 Güvenlik özelliklerinin yönetimi

Açıklama: Güvenlik özelliklerinin yönetimi, yetkili kullanıcıların(rollerin) belirlenen güvenlik değerlerini kontrol etmelerine izin verir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: [FDP_ACC.1 Erişim kontrolünün alt seti veya

FDP_IFC.1 Bilgi akış kontrolünün alt seti

FMT_SMR.1 Güvenlik rolleri

FMT_SMF.1 Yönetim fonksiyonlarının özellikleri

FMT_MSA.1.1 TSF [Sistem Yöneticisi] için [*sorgu*] güvenlik nitelikleriyle [FAU_GEN.1 oluşturulan kayıtları] [FDP_ACC.1 erişim denetim(ler)i ve FDP_IFC.1 bilgi akışı kontrol (ler)] yeteneğini kısıtlamak zorundadır.

FMT_MSA.3 Statik Nitelik Başlatma

Açıklama: Statik nitelik başlatılması sırasında değerlerin uygun olduğundan emin olunur.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FMT_MSA.1 Güvenlik özelliklerinin yönetimi

FMT_SMR.1 Güvenlik rolleri

FMT_MSA.3.1 TSF SFP uygulamak için kullanılan güvenlik özellikleri için [*kısıtlayıcı]* varsayılan değerler sağlamak için [SFP erişim kontrol , SFP bilgi akış kontrolü] yürütür.

FMT_MSA.3.2 TSF [Sistem Yöneticisi] bir nesne ya da bilgi oluşturulduğunda, varsayılan değerleri geçersiz kılmak için alternatif başlangıç değerlerini belirtmek için izin verecektir.

6.1.5.3 FMT_MTD.1 TSF Veri Yönetimi

Açıklama: TSF veri yönetimi yetkili kullanıcıların TSF verilerini yönetmek için izin verir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FMT_SMR.1 Güvenlik rolleri

FMT_SMF.1 Yönetim Fonksiyonları Özellikleri

FMT_MTD.1.1 [Sistem Yöneticisi] için [FAU_GEN.1 tarafından üretilen kayıtlar] için [*sorgu*] yeteneğini kısıtlamak zorundadır.

6.1.5.4 FMT_SAE.1 Zaman-Limitli Yetkilendirme

Açıklama: Zaman-limitli yetkilendirme, belirlenen güvenlik özelliklerinin yetkili kullanıcılar tarafından zaman aşımı değerlerinin belirlenmesini sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FMT_SMR.1 Güvenlik Rolleri

FPT_STM.1 Zaman Damgası

FMT_SAE.1.1 TSF [Sistem Yöneticisi] için [FIA_SOS.2 tarafından üretilen mesaj] için bir sona erme zamanı belirtmek için yeteneği kısıtlamak zorundadır.

FMT_SAE.1.2 Bu güvenlik niteliklerin her biri için, TSF belirtilen güvenlik özelliği için sona erme süresi sonrasında [Kullanıcı Yeniden-Yetkilendirme] mümkün olacaktır.

6.1.5.5 FMT_SMF.1 Belirlenmiş Yönetim Fonksiyonları

Açıklama: TSF tarafından sağlanan belirlenmiş yönetim fonksiyonları

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FMT_SMF.1.1 Aşağıdaki yönetim fonksiyonları TSF tarafından yapılır: [TSF tarafından sağlanan yönetim fonksiyonları listesi].

6.1.5.6 FMT_SMR.1 Güvenlik Rolleri

Açıklama: TSF tarafından kullanılacak güvenlik rolleri tanımlanır.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: FIA_UID.1 Tanımlama Zamanlaması

FMT_SMR.1.1 TSF rollerin yönetimini bu rolle sağlar. [Sistem Yöneticisi].

FMT_SMR.1.2 TSF Kullanıcı ve rollerle ilişkisini sağlar.

SFR	Yönetim Olayları	Ayrıntılı Bilgi
FMT_MOF.1	Fonksiyon davranışlarının değiştirilmesi, aktifleştirilmesi, pasifleştirilmesi	Web Servis ve Tanımlama
FMT_MSA.1	Güvenlik özellikleri ve aksiyonlar	Tanımlı erişim kayıtları ve bilgi akış kontrolleri
FMT_MSA.3	Static özellik başlangıç olayları	Belirtilmiş alternatif başlangıç değerleri
FMT_MTD.1	TSF Veri Yönetim olayları	
FMT_SAE.1	Zaman limitli yetkilendirme	FIA_SOS.2 üretilmiş mesaj
FMT_SMF.1	Yönetim fonksiyonlarının özellikleri	Yönetim fonksiyonlarının listesi
FMT_SMR.1	Güvenlik rolleri	

6.1.6 TSF Koruma Sınıfı (FPT)

6.1.6.1 FPT_STM.1 Zaman Damgası

Açıklama: TSF fonksiyonları için TSF tarafından sağlanan zaman damgasını tanımlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FPT_STM.1.1 TSF erişilebilir zaman damgasını sağlar.

6.1.7 Kaynak Kullanım Sınıfı (FRU)

6.1.7.1 FRU_RSA.1 Maksimum Kota

Açıklama: Maksimum kota, kaynakların kullanıcı ve özneler tarafından düzgün bir şekilde kullanılması için gerekli kota yönetimini sağlar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FRU_RSA.1.1 TSF [*Web Servis Fonksiyonlarının*] [*eş zamanlı*] olarak kullanılması sırasında [XML Mesaj] kaynağı üzerinde maksimum kotaya göre kulanımı zorlamalıdır.

6.1.8 Güvenli Yol/Kanallar Sınıfı (FTP)

6.1.8.1 FTP_ITC.1 Dahili-TSF güvenli kanal

Açıklama: Dâhili-TSF güvenli kanal, TSF' in kendisi ve başka bir IT ürünü ile güvenli bir iletişim kanalı sağlamasını gerekli kılar.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FTP_ITC.1.1 TSF kendisi ve diğer güvenilir IT ürünü arasında güvenli bir iletişim kanalı sağlar. Bu mantıksal olarak farklı bir uç nokta ile iletişim sırasında verinin gizli kalmasını ve değiştirilmesini önleyecek gerekli korumayı ve yetkilendirmeyi içerir.

FTP_ITC.1.2 TSF,[*TSF*] tarafından güvenli kanal üzerinden iletişimin başlatılmasına izin verir.

FTP_ITC.1.3 TSF [Kullanıcı Tanımlama, Yetkilendirme ve Web Servis Erişimi] için iletişimi güvenli kanal üzerinden başlatmalıdır.

6.1.8.2 FTP_TRP.1 Güvenli Yol

Açıklama: Güvenli yol, PP/ST yetkilisi tarafından tanımlanmış olaylar kapsamında TSF tarafından kullanılacak güvenli yolu gerekli kılar. TSF ve/vay kullanıcı bu güvenli yolun hazırlanmasını sağlayabilir.

Hiyerarşi: Başka bileşenlerle ilişkisi bulunmamaktadır.

Bağımlılık: Herhangi bağımlılığı bulunmamaktadır.

FTP_TRP.1.1 TSF kendisi ve [*yerel ve uzak*] kullanıcılar arasında mantıksal olarak farklı bir uç nokta ile yapacağı iletişim sırasında iletişim yapılan verinin [*gizli*] kalmasını sağlayacak güvenilir yolu sağlar.

FTP_TRP.1.2 TSF güvenli yol üzerinden [*yerel kullanıcılar ve uzak kullanıcılar*] tarafından iletişim başlatılmasına izin verir.

FTP_TRP.1.3 TSF belirlenen güvenli yolun kullanılmasını gerekli kılar. [*başlangıç kullanıcı yetkilendirme* [Web Servis Erişimi]].

6.2 TOE için Güvenlik Güvence Gereksinimleri

TOE kapsamında değerlendirme için gerekli geliştirme ve işletme operasyonlarına ilişkin güvenlik güvence gereksinimleri ön tanımlı EAL2 tanımlarından seçilmiştir.

6.3 Güvenlik Gereksinimleri İlişkileri

6.3.1 Güvenlik Fonksiyonel Gereksinimleri İlişkileri

		O.ACCONTROL	O.VALAUTH	O.INTEGRITY	O.RECORDS	O.AUTHORIZE
GÜVENLİK DENETİMİ	FAU_GEN.1				**X**	
	FAU_GEN.2	**X**			**X**	**X**
	FAU_SAR.1	**X**			**X**	**X**
	FAU_SEL.1	**X**			**X**	**X**
	FAU_STG.1				**X**	**X**
İLETİŞİM	FCO_NRO.1		**X**	**X**		
	FCO_NRR.1		**X**	**X**		
KULLANICI VERİSİ KORUMA	FDP_ACC.1	**X**				
	FDP_ACF.1	**X**	**X**			**X**
	FDP_DAU.1		**X**			**X**
	FDP_IFC.1		**X**	**X**	**X**	
	FDP_IFF.1		**X**	**X**	**X**	
TANIMLAMA VE YETKİLENDİRME	FIA_AFL.1					**X**
	FIA_ATD.1					**X**
	FIA_SOS.1		**X**			
	FIA_SOS.2		**X**	**X**		
	FIA_UAU.1					**X**
	FIA_UAU.6		**X**			**X**
	FIA_UID.1					**X**
GÜVENLİK YÖNETİMİ	FMT_MOF.1	**X**	**X**			**X**
	FMT_MSA.1					**X**
	FMT_MSA.3	**X**				**X**
	FMT_MTD.1	**X**	**X**			**X**
	FMT_SAE.1	**X**	**X**			
	FMT_SMF.1	**X**				
	FMT_SMR.1		**X**			**X**
TSF KORUMASI	FPT_STM.1				**X**	
KAYNAK FAYDALANMASI	FRU_RSA.1	**X**		**X**		
GÜVENLİ YOL / KANALLAR	FTP_ITC.1			**X**		**X**
	FTP_TRP.1					**X**

GÜVENLİK NESNELERİ	GÜVENLİK FONKSİYONEL GEREKSİNİMLERİ	
O.ACCONTROL	FAU_GEN.2	Kullanıcı kimliği ile ilişkiyi sağlar.
	FAU_SAR.1	Denetim kayıtları için okunacak bilgilerin kapasitesini sağlar.
	FAU_SEL.1	Tüm denetim olaylarından denetlenecek olayların seçilmesini sağlar.
	FDP_ACC.1	Veri ve fonksiyonlar için güvenlik fonksiyon politikasını sağlar.
	FDP_ACF.1	Güvenlik özellikleri ve tanımlandırılmış güvenlik özellik gruplarına göre erişimi zorunlu kılar.
	FMT_MOF.1	Yetkilendirilmiş kullanıcılar tarafından belirlenen kullanım kuralları ve tanımlı şartlar çerçevesinde güvenlik fonksiyonlarının davranışlarının yönetimine izin verir.
	FMT_MSA.3	Güvenlik özelliklerinin static değerlerinin verildiğinden emin olur.
	FMT_MTD.1	Veriler ve olay verileri ile ilgili yetkilendirilmiş işlemleri sağlar.
	FMT_SAE.1	Belirlenmiş güvenlik özelliklere göre yetkilendirilmiş kullanıcılar için zaman aşımı süresinin tanımlanmasını sağlar.
	FMT_SMF.1	Sadece bakım modunda izin verilen işlemleri onaylar.
	FRU_RSA.1	Kontrol edilen kaynaklara yönelik olarak kullanıcı ve öznelerin kullanımı sırasında gerekli olan kota mekanizmasını sağlar.
O.VALAUTH	FCO_NRO.1	Bilginin alışverişi sırasında göndericinin TSF tarafından seçilebilmesini gerekli kılar.
	FCO_NRR.1	Bilginin alışverişi sırasında alıcının TSF tarafından seçilebilmesini gerekli kılar.
	FDP_ACF.1	Güvenlik özellikleri ve tanımlandırılmış güvenlik özellik gruplarına göre erişimi zorunlu kılar.
	FDP_DAU.1	TSF tarafından Nesnelerini bilgi içeriklerinin erişilebilmesi için gerekli yetkilendirilmenin garanti altına alınmasını sağlar.
	FDP_IFC.1	Veriler ve olay verileri için bilgi akış kontrolünü sağlar.
	FDP_IFF.1	Veri için bilgi akış kontrolünü sağlar.
	FIA_SOS.1	Tanımlı kalite metrikleri çerçevesinde güvenlik mesajlarının doğrulanmasını gerekli kılar.
	FIA_SOS.2	Tanımlı kalite metrikleri çerçevesinde güvenlik mesajlarının üretilmesini gerekli kılar.
	FIA_UAU.6	Belirlenen olaylar kapsamında kullanıcılar tarafından ihtiyaç duyulacak yeniden yetkilendirmeyi gerekli kılar.
	FMT_MOF.1	Yetkilendirilmiş kullanıcılar tarafından belirlenen kullanım kuralları ve tanımlı şartlar çerçevesinde güvenlik fonksiyonlarının davranışlarının yönetimine izin verir.
	FMT_MTD.1	Veriler ve olay verileri ile ilgili yetkilendirilmiş işlemleri sağlar.
	FMT_SAE.1	Belirlenmiş güvenlik özelliklerine göre yetkilendirilmiş kullanıcılar için zaman aşımı süresinin tanımlanmasını sağlar.
	FMT_SMR.1	TSF tarafından değerlendirilecek güvenlik rollerinin belirlenmesini sağlar.
O.INTEGRITY	FCO_NRO.1	Bilginin alışverişi sırasında göndericinin TSF tarafından seçilebilmesini gerekli kılar.
	FCO_NRR.1	Bilginin alışverişi sırasında alıcının TSF tarafından seçilebilmesini gerekli kılar.
	FDP_IFC.1	Veri için bilgi akış kontrolünü sağlar.
	FDP_IFF.1	Veri için bilgi akış kontrolünü sağlar.

O.INTEGRITY	FIA_SOS.2	Tanımlı kalite metrikleri çerçevesinde güvenlik mesajlarının üretilmesini gerekli kılar.
	FRU_RSA.1	Kontrol edilen kaynaklara yönelik olarak kullanıcı ve öznelerin kullanımı sırasında gerekli olan kota mekanizmasını sağlar.
	FTP_ITC.1	TOE ve diğer başka bir IT ürünü arasındaki TSF tarafından sağlanan güvenli iletişim kanalını gerekli kılar.
O.AUTHORIZE	FAU_GEN.2	Kullanıcı kimliği ile ilişkiyi sağlar.
	FAU_SAR.1	Denetim kayıtları için okunacak bilgilerin kapasitesini sağlar.
	FAU_SEL.1	Tüm denetim olaylarından denetlenecek olayların seçilmesini sağlar.
	FAU_STG.1	Denetim kayıtlarını yetkisizi bir şekilde silinmesine karşın saklar.
	FDP_ACF.1	Güvenlik özellikleri ve tanımlandırılmış güvenlik özellik gruplarına göre erişimi zorunlu kılar.
	FDP_DAU.1	TSF tarafından Nesnelerini bilgi içeriklerinin erişilebilmesi için gerekli yetkilendirilmenin garanti altına alınmasını sağlar.
	FIA_AFL.1	Yetkilendirme hata olaylarının tespit edilmesi ve kayıt edilmesini sağlar.
	FIA_ATD.1	Herhangi bir kullanıcı güvenlik değerinin bakımına izin verir.
	FIA_UAU.1	Herhangi bir aksiyon yapılmadan önce gerekli kullanıcı yetkilendirmesini tanımlar.
	FIA_UAU.6	Belirlenen olaylar kapsamında kullanıcılar tarafından ihtiyaç duyulacak yeniden yetkilendirmeyi gerekli kılar.
	FIA_UID.1	Tanımlı yapılmadan herhangi bir aksiyona izin vermez.
	FMT_MOF.1	Yetkilendirilmiş kullanıcılar tarafından belirlenen kullanım kuralları ve tanımlı şartlar çerçevesinde güvenlik fonksiyonlarının davranışlarının yönetimine izin verir.
	FMT_MSA.1	FCR yetkilendirilmiş kullanıcıların güvenlik özelliklerinin değiştirilmesinin kısıtlayan fonksiyonlar sağlar.
	FMT_MSA.3	Güvenlik özelliklerinin static değerlerinin verildiğinden emin olur.
	FMT_MTD.1	Veriler ve olay verileri ile ilgili yetkilendirilmiş işlemleri sağlar.
	FMT_SMR.1	TSF tarafından değerlendirilecek güvenlik rollerinin belirlenmesini sağlar.
	FTP_ITC.1	TOE'nin kendisi ve başka bir IT ürünü ile iletişimi için güvenli bir iletişim kanalını gerekli kılar.
	FTP_TRP.1	PP/ST yetkilisi tarafından tanımlanan ve kullanıcı ile TSF arasındaki güvenli bir yolun olmasını gerekli kılar.
O.RECORDS	FAU_GEN.1	Doğru denetim olaylarını üretir
	FAU_GEN.2	Kullanıcı tanımlama ilişkisini sağlar.
	FAU_SAR.1	Denetim kayıtlarının kullanıcılar tarafından okunabilmesini sağlar.
	FAU_SEL.1	Tüm denetim olaylarından denetlenecek olayların seçilmesini sağlar.
	FAU_STG.1	Denetim kayıtlarını yetkisizi bir şekilde silinmesine karşın saklar.
	FDP_IFC.1	Veriler ve olay verileri için bilgi akış kontrolünü sağlar.
	FDP_IFF.1	Veri için bilgi akış kontrolünü sağlar
	FPT_STM.1	Olayların kaydı için gerekli olan zaman bilgisini sağlar

6.3.2 Güvenlik Güvence Gereksinimleri İlişkisi

Geçerli güvence paketi olarak önceden tanımlanmış EAL2 paketi seçilmiştir. EAL2 seçilme nedeni ise geliştirilen Web Servis teknolojileri için oluşabilecek tehditlerin bir saldırgan için temel atak potansiyeli içermesidir.

6.3.3 Güvenlik Gereksinimleri- İç Tutarlılık

Güvenlik gereksinimlerinin mantığı aşağıdaki güvenlik fonksiyonel gereksinimleri (SFRs) ve güvence gerekliliklerinden (SARs) oluşan TOE için güvenlik gereksinimleri seti ile birlikte tutarlı bir bütün olduğunu gösterir.

EAL 2 Güvence paketi tutarlı bir şekilde daha önceden tanımlanmış bir settir. Güvence gereksinimleri ve bağlı olan tüm bağımlılıkları arasında herhangi bir tutarsızlık olmayacak şekilde belirlenmiştir. Fonksiyonel ve güvence arasındaki tutarsızlık sadece fonksiyonel-güvence bağımlılıkları sağlanmadığı zaman ortaya çıkar. Bundan dolayı, güvenlik gereksinimlerinin iki grubu arasında herhangi bir tutarsızlık bulunmamaktadır.

7. KISALTMALAR

CC	Ortak Kriterler
EAL	Değerlendirme Güvence Seviyesi
IT	Bilgi Teknolojisi
OSP	Kurumsal Güvenlik Politikası
PP	Koruma Profili
SAR	Güvenlik Güvence Gerekleri
SFR	Güvenlik Fonksiyonel Gerekleri
SSL	Güvenli Soket Katmanı
TOE	Değerlendirme Hedefi
TSF	TOE Güvenlik Fonksiyonalitesi

8. KAYNAKLAR

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

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

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

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

[5] SANS, XML Web Services Security and Web based Application Security, Chris Kwabi, GIAC Security Essentials Certification Practical Assignment Version 1.4b, Website URL: http://www.sans.org/reading-room/whitepapers/securecode/xml-web-services-security-web-based-application-security-1201

[6] OWASP, Web Services Architecture and Security, Website URL: https://www.owasp.org/index.php/Web_Services_Architecture_and_Security

[7] OWASP**,** Web Service Security Cheat Sheet, Website URL: https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet