Security Information and Event Management Systems Protection Profile

Version 1.0

TURKISH STANDARDS INSTITUTION

July 2014

İÇİNDEKİLER

DEFINITIONS AND ABBREVIATIONS

Assets: Information or resources to be protected by the countermeasures of a TOE.

Assignment: The specification of an identified parameter in a component (of the CC) or requirement.

Attack: An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.

Attack Potential: A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Audit Trail: In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authentication: To establish the validity of a claimed user or object.

Authentication Data: Information used to verify the claimed identity of a user.

Authorized Administrator: An authorized user who may, in accordance with the SFRs, operation and manage Firewall.

Authorized User: A user who may, in accordance with the SFRs, perform an operation.

Availability: Assuring information and communications services will be ready for use when expected.

Class: A grouping of CC families that share a common focus.

Common Criteria (CC): The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs), vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

Component: The smallest selectable set of elements on which requirements may be based.

Confidentiality: Assuring information will be kept secret, with access limited to appropriate persons.

Dependency: A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Electronic Seal (e-Seal): A type of electronic signature, which uses the same technology with electronic signature and can be issued for organizations, rather than individuals. Electronic seal shall be seen as a supplementary of electronic signature, not an alternative.

Electronic Signature (e-Signature): Binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document or message.

Element: An indivisible statement of security need.

Evaluation Assurance Level (EAL): An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External Entity: any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family: A grouping of components that share a similar goal but may differ in emphasis or rigor.

Identity: A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity: Assuring information will not be accidentally or maliciously altered or destroyed.

Intrusion: Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection: Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

Iteration: The use of the same component to express two or more distinct requirements.

Metadata: This is information about documents or records. It is either automatically generated when a document is created or it may require the user to fill in some fields. For example the metadata for a word document might include title, author, date created etc.

Object: A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation (on a component of the CC): Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object): A specific type of action performed by a subject on an object.

Organizational Security Policy (OSP): A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Protection Profile (PP): An implementation-independent statement of security needs for a TOE type.

Qualified Certificate: Qualified Certificate that is suitable with electronic signatures law of Turkey (Electronic Signature Law numbered 5070).

Refinement: The addition of details to a component.

Role: A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security Assurance Requirement (SAR): descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.

Security Functional Requirement (SFR): Specification of individual security functions which may be provided by a product.

Security Function Policy (SFP): A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Target (ST): An implementation-dependent statement of security needs for a specific identified TOE.

Selection: The specification of one or more items from a list in a component.

SIEM: SIEM is a centralized software or appliance which gathers data generated by different multi-vendor security and/or system devices; normalizes, stores and then filters and correlates these data according to rules created by users.

SIEM Data: Data collected by the SIEM functions

SIEM Functions: The active part of the SIEM responsible for performing correlation analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.

Subject: An active entity in the TOE that performs operations on objects.

Target Of Evaluation (TOE): A set of software, firmware and/or hardware possibly accompanied by guidance.

Threat: The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

Threat Agent: An unauthorized user that brings assets under such threats as illegal access, modification or deletion.

TOE Security Functionality (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

TSF Data: Data created by and for the TOE, that might affect the operation of the TOE.

Turkish Standards Institution (Türk Standardları Enstitüsü - TSE): TSE has been established by the law numbered 132 dated 18.11.1960 for the purpose of preparing standards for every kind of item and products together with procedure and service. The Institute is responsible to the Prime Ministry. The Institute is a public founding which is conducted according to the special rules of law and has a juristic personality. Its abbreviation and trademark is TSE.

User: See definition of “external entity”

Vulnerability: Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Workflow: Automation of business processes, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.

1. PROTECTION PROFILE INTRODUCTION

1.1. REFERENCE

Reference information of this protection profile is shown in the table below.

Protection Profile Name	Security Information and Event Management Systems Protection Profile
Document Version	1.0
Publication Date	2014-07-24
Conforming CC Version	CC v3.1 Revision 4
Conforming EAL	EAL 4
Developers	Turkish Standards Institution
Sponsor	Turkish Standards Institution, Turkey
Keywords	Security Event Management, Security Information Management, Log Analyzer, Log Management, analysis, correlation, SEM, SIM, SIEM.

1.2. DEFINITION OF AIMS AND SCOPE

In National Cyber Security Strategy and Action Plan, which went in effect by being published Turkish Official Gazette dated 06/20/2013 and numbered 28683, in the direction of Council of Ministers Decision numbered 2013/4890, TSE was assigned to prepare national standards in the field of information security. Within this scope, National Cyber Security Specialists Committee has been formed under the administration of TSE and standards and guidance documents have been prepared in a wide range of technical topics. This protection profile is one of the outputs of these efforts. All outputs of National Cybersecurity Specialists Committee are listed under http://bilisim.tse.org.tr (turkish).

Log yönetimi, kuruluşların temel vazifelerinden birisi haline gelmiştir. Kamu kurumları ve özel sektör kuruluşları tarafından sürdürülen bilişim altyapıları her geçen gün daha da büyümekte, kuruluşlar bünyesinde kurulan bilgi sistemleri nicelik ve nitelik açısından giderek artmaktadır. Gerek mevzuat yükümlülükleri, gerekse artan güvenlik ihtiyacı sebebiyle kuruluşlar bilişim sistemleri üzerinde tutulan log kayıtlarını daha detaylı inceleme ve bu kayıtlara bütüncül bakabilme yeteneğine sahip olma eğilimindedir. Bu çalışma, söz konusu ihtiyaç çerçevesinde, kurumsal bilgi sistemlerinde tutulan günlük kayıtlarının merkezi olarak toplanması, analizi, çapraz kontrollere tabi tutulması gibi işlevleri gerçekleştiren Merkezi Log Yönetimi ve Korelâsyon yazılımlarına yönelik olarak hazırlanmış olup bu yazılımların güvenliğinin teminine yöneliktir.

Güvenlik olaylarının tespiti ve engellenmesi için yaygın olarak kullanılan IDS/IPS sistemleri, günümüzde tek başına yeterli olmamakta, bu cihazlar tarafından oluşturulan gerçeğe aykırı doğru (false-positive) alarmlar kuruluşların güvenlik süreçlerinde aksamalara neden olabilmektedir. MLYS yazılımı birden fazla noktadan sistem ve güvenlik günlüklerini merkezi bir sistemde toplayıp düzenleyerek ilişkilendirir ve gerçeğe aykırı doğruları azaltıp anlamlı veriyi oluşturmaya yarar. Bu süreç içerisinde IDS/IPS tarafından sağlanan log kayıtları kullanılabileceği gibi, farklı her türlü kaynaktan da günlük kayıtları toplanabilir.

Bu koruma profilinin yapısı gereği, sertifikasyon değerlendirmesine tabi tutulacak BT ürün grubuna değerlendirme hedefi (Target of Evaluation, TOE) adı verilmektedir. Sistem güvenliğinin etkin bir şekilde sağlanabilmesi için, BT ortamında bulunup TOE' nin güvenlik fonksiyonlarıyla ilişkili olan tüm cihazlar en azından TOE' nin güvenilirlik seviyesinde olmalıdırlar. Ancak TOE ile ciddi anlamda iç içe çalışan sistem bileşenleri de, TOE' nin üzerinde koştuğu

işletim sistemi gibi, uygun bir koruma profiliyle değerlendirilebilir. TOE' nin yönettiği verilerin bütünlük ve gizliliği kurumlar için elzem olduğundan, sadece TOE üzerinde uygulanmış güvenlik önlemleri yeterli nitelikte bir güvenlik derecesini sağlayabilmek için yeterli olmayacaktır.

1.3. TOE OVERVIEW

1.3.1. INTRODUCTION

TOE ilgili denetim/iz [MRÖ1]kayıtlarını bulunduğu ortam ve bu ortama bağlı bileşenlerden toplar; düzenler, süzer ve olay ilişkilendirme kuralları uygulayarak bu veriler arasındaki ilişkileri inceler. Bu verileri kullanıcıya gösterirken hızlı arama, detaylı arama, filtreleme gibi özellikler sunar. TOE gerçek zamanlı ve/veya[MRÖ2] kronolojik olarak denetim/günlük kayıtlarını düzenler, ilişkilendirir ve raporlar. TOE' nin kendi denetim kaydını tutma özelliği de vardır. Denetim/günlük kayıtlarının alındığı cihazlar [MRÖ3]yerel ağ ile erişilen cihazlar olabileceği gibi, harici bir konumda da bulunabilir.

Denetim/günlük kayıtlarının yanı sıra NetFlow, sFlow, packet capture gibi verilerin de analizine de imkân veren TOE alternatifleri bulunmaktadır. Analiz edilen veriler ağ/bilgi güvenliği olay yönetimi, kullanıcı aktivite yönetimi, kronolojik analiz ve uyumluluk raporları gibi farklı amaçlar için kullanılabilir. Analizler hem gerçek zamanlı, hem de kronolojik gerçekleştirilebilir. TOE, güvenlik raporları oluşturabilir; bu raporların PDF, CSV gibi formatlarda dışarı aktarılmasına izin verir.

TOE kurallar, tetikler ve eşik değerleri oluşturmak suretiyle olası saldırılara karşı tedbir alınmasını sağlar. Günün belirli saatlerinde, haftanın belirli günlerinde farklı kurallar hayata geçirilebilir. TOE tetikleri ve alarmları tanımlar; bu tetik ve alarmlar için kuralları belirler. Bu kurallar azami yetkisiz erişim sayısı olabileceği gibi, bir sistem üzerinde oluşturulan kullanıcı hesabı sayısı, aktarılan trafiğin miktarı, ağ/sistem aykırılıkları gibi pek çok farklı konu olabilir. Kurallar belirlendikten sonra, bu kurallara uyan herhangi bir olay meydana geldiğinde, TOE daha önceden tanımlanmış olan eylemi veya eylemleri hayata geçirir. Bu eylemler, önceden belirlenmiş adreslere elektronik posta yollama; komut ya da script/komut çalıştırma gibi eylemler olabilir. TOE sunucuyu kapatmak, kullanıcının oturumunu sonlandırmak, sistem yöneticisini bilgilendirmek, kullanıcıyı bilgilendirmek, işlemi sonlandırmak, kullanıcı hesabını sıfırlamak gibi bazı karşı önlemleri otomatik bir şekilde hayata geçirebilir.

TOE ağa bağlı bir cihaz üzerine kurulu bir yazılımdan veya birbirine bağlı farklı donanım bileşenlerinin üzerine kurulu ve birbiriyle iletişim halindeki yazılımlardan oluşur ve aynı zamanda bir altyapı bileşenidir. TOE ajanlı ya da ajansız olarak kuruluma imkân vermelidir. TOE fiziksel ya da sanal sunucularda da kurulabilmelidir. TOE' ye sistem kullanıcıları tarafından erişim grafiksel kullanıcı arayüzü (GUI) ve/veya komut satırı arayüzü (CLI) aracılığıyla yapılır. GUI ile yapılan tüm işlemler CLI ile de yapılabilmelidir. [FB4]GUI ya da CLI' ya erişim şifrelenmiş olmalıdır. (Web tabanlı GUI için https; CLI için ssh gibi). Kullanıcılar GUI ya da CLI için aynı yetkilere sahip olmalıdır. TOE yerel ve uzaktan kimlik doğrulama ve yetkilendirme işlemlerine imkân tanır. TOE denetim/günlük kayıtlarını kimlik doğrulanmış ya da kimlik doğrulanmamış olarak toplayabilir. Örneğin OPSEC kimlik doğrulama gerektiren bir protokol iken Syslog UDP 514 portundan kimlik doğrulama olmadan denetim/günlük kaydı gönderebilir. TOE' ye yapılan güncellemelerin kaynağı doğrulanır ve bu güncellemelerin güvenli bir şekilde yapılması sağlanır.

Bu koruma profilinin kullandığı protokoller elektronik sertifikaları kullanır, ama sertifika altyapısına ilişkin protokolleri (örneğin OCSP protokolü) barındırmaz. Bunlar daha sonraki sürümlerde eklenecektir. Kolay uygulanabilir, basit bir koruma profili hazırlanmıştır.

MLYS, güvenlik bakış açısıyla bir kurumun en kritik varlıklarından birisidir. Bu nedenle, bu bileşen kritik varlıklar arasına dâhil edilmeli ve doğru ve etkin bir şekilde çalıştığından emin olunmalı, düzenli olarak testlerden geçirilmelidir. Ayrıca MLYS'in üzerinde çalıştığı yazılım ve donanım katmanları yüksek risk taşıyan bileşenler kategorisinde olacak şekilde yapılandırılmalıdır.

İçişleri Bakanlığının dokümanında belirtilen "İz Kaydı Alınması Gereken Sistemler"e ilave olarak diğer sistemlerden de (kullanıcı terminalleri, balküpü sistemi, veri kaçağı önleme sistemi, URL filtreleme vb.) iz kaydı alınması tavsiye edilir.

- İçişleri Bakanlığının "olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari nitelikleri" dokümanına atıf.[FB5]

1.3.2. TOE TYPE

TOE is a "security information and event management software", which is connected to network infrastructure and components.

1.3.3. TYPE OF USERS

Temel olarak üç farklı kategoride kullanıcı tipi bulunmaktadır. Bunlar;

- Normal Kullanıcı
- Yönetici
- Süper_Yönetici[MRÖ1]

Yukarıda bahsi geçen rollere ek olarak TOE üzerinde daha farklı rollere sahip kullanıcılar oluşturulabilir. ST yazarı tarafından farklı rollere ihtiyaç duyulması halinde bu roller burada listelenip açıklanmalıdır.

Normal Kullanıcı: Normal kullanıcı TOE üzerinde salt okunur erişim hakkına sahip kullanıcı tipidir. Normal kullanıcı arama, listeleme ve rapor alma gibi işlemleri gerekli yetki verildiği takdirde yapabilir. Herhangi bir kaydı silemez ve kullanıcı hesapları üzerinde herhangi bir işlem yetkisi yoktur. Olay günlükleri ve raporlar üzerinde sadece salt okunur erişim hakkı bulunmaktadır.

Yönetici: Yöneticiler TOE' yi kurallar, filtreler ve veri yönetimi safhalarında yönetir ve bu yolla kurumsal güvenlik kuralları ve uygulamalarının denetlenmesini/teyit edilmesini sağlar. Yöneticilerin TOE' yi analiz ve operasyon safhalarında yönetmek ve birçok TSF verisini sorgulayıp düzenlemek adına yetkileri vardır. Ancak yöneticiler kullanıcı hesaplarını oluşturamaz veya değiştiremez.

Süper_Yönetici: Süper_Yönetici TOE' nin tüm yönleriyle yönetilebilmesi için gerekli yetkilere sahiptir. Süper_Yöneticiler TOE üzerinde en yetkin haklara sahiptirler. Ayrıca Süper_Yönetici kullanıcı hesaplarını ve haklarını oluşturabilir, değiştirebilir ve/veya silebilir.

Kullanıcı tipleri bir ya da birkaç kişiden oluşabilir ya da TOE' nin çeşitli bölümleri için özgün kullanıcı tipleri tanımlanabilir.

1.3.4.3. MAIN SECURITY FEATURES OF THE TOE

Kimlik Doğrulama ve Yetkilendirme:

TOE kullanıcıları kendilerine verilen yetkileri kullanabilmek için benzersiz bir kullanıcı adı ve şifreyle TOE' ye erişim sağlamalıdırlar. Kimlik doğrulama esnasında eğer geçerli kimlik bilgileri sağlanmışsa kullanıcıya özgü yetkilendirme yapılır ve bağlantı kurulur. Eğer girilen kimlik bilgileri geçersizse erişim reddedilir ve bağlantı kesilir. Kullanıcı önceden belirlenmiş bir eşik süresi kadar işlem yapmazsa bağlantı kesilir ve kullanıcı oturum açma ekranına yönlendirilir. TOE, kullanıcı yetkilerini kullanıcının yaptığı her işlem başlangıcında kontrol eder. Eğer bir oturum esnasında/oturum sürerken kullanıcı yetkileri değişirse bu değişiklik kullanıcının bir sonraki işleminde hayata geçirilir. TOE kullanıcı kimliklerini, kimlik doğrulama verilerini, yetkilendirme bilgilerini ve bu yetkilere sahip rolleri kayıt altına alır.

Erişim Kontrolü:

TOE denetim kayıtlarına erişimi farklı kaynaklardan erişim anlamında kısıtlayabilir. TOE yetkilendirilmiş kullanıcıları kaynak IP adresine göre kısıtlayabilir. Daha ileri düzey kısıtlamalar kullanıcıların erişim hakları yanında oturumların zaman aralıkları ve IP adreslerine göre de yapılabilir.

Denetim:

TOE aşağıda belirtilen denetim kayıtlarını toplayabilmelidir.

- TOE' nin tüm servislerinin açılıp kapanması,
- TOE' nin denetim kayıtlarına başarılı ve başarısız olarak gerçekleştirilen analiz erişimleri
- TOE' nin yapılandırma dosyaları üzerinde farklı kullanıcılar tarafından gerçekleştirilen değişiklikler,
- Tüm kimlik ve kimlik doğrulama kaynakları,
- TOE' ye erişim, TOE tarafından toplanan günlük kayıtları ve TOE tarafından tespit edilen olaylar,
- TOE' nin güvenlik yapılandırma fonksiyonları üzerinde yapılan değişiklikler,
- TOE' nin güvenlik yapılandırma fonksiyon verileri üzerinde yapılan değişiklikler,
- TOE' nin kullanıcı erişim/yönetim profili üzerinde yapılan değişiklikler,

Tüm denetim kayıtları herhangi bir değişiklik ya da silinmeye karşı korunmalıdır.

Tüm denetim olaylarına ait veriler uygun bir karıştırma (hashing) algoritmasıyla karıştırılarak bir karıştırma imzası oluşturulur ve bu imza denetim kayıtlarına eklenir. Her bir denetim iz kaydı;

- Olayın tarih ve zamanı, denetim kayıtları için yetkilendirilmiş bir kuruluştan zaman damgası alınabilmesi için harici bir bağlantı gerektirebilir.
- Sistem ya da kullanıcı tarafından talep edilen işlem,
- İşlemi gerçekleştiren kullanıcı adı,
- Olay verisine ait dosya adı ve olayın başarılı ya da başarısız olarak gerçekleştiği bilgisi,
- Denetim kayıtlarındaki herhangi bir aykırılığı tespit etmeye yarayan, olaya verilen sırasal bir ID,
- Zaman damgası ve ID içeren karıştırma tabanlı bir imza.

TOE yetkilendirilmiş kullanıcılara olay verilerini alma, denetim kayıtlarını olay türü ve çeşitli alanlara göre sıralama imkânı verir. TOE denetim kayıtlarına yetkisiz erişimleri engellemek adına farklı arayüzlerine sınırlı erişim hakkı verir.

TOE, diğer bileşenlerle ilgili denetim kayıtlarını analiz ederken, bir taraftan kendi üzerinde yapılan işlemlerin de denetim kayıtlarını oluşturur.

Güvenlik Yönetimi:

TOE yetkilendirilmiş kullanıcılara, TOE fonksiyonlarını ayarlama ve güncelleme için bir grafiksel kullanıcı arayüzü (GUI) sağlar. Bu arayüz genellikle bir web arayüzü olmakla birlikte, doğrudan internete açık değildir. GUI tarafından kontrol edilen fonksiyonlar; denetim fonksiyonlarını, kullanıcı hesaplarını ve denetim verilerini kullanıcıların yetkilerine göre yönetme imkânı sağlar. TOE ayrıca yukarıda bahsi geçen fonksiyonları yönetmek için bir komut satırı arayüzüne (CLI) de imkân verebilir.

TOE Bölüm 1.3.3 de açıklanan kullanıcı tiplerine göre yönetim rollerinin uygulanmasını sağlar ve her bir kullanıcının TOE' ye erişirken kendi yetkileriyle işlem yapmasını güvence altına alır. Süper_Yöneticiler ve Yöneticilerin, TOE' yi analiz ve operasyon safhalarında yönetmek ve birçok TSF verisini sorgulayıp düzenlemek adına yetkileri vardır. Normal kullanıcılar denetim verisi/günlük kayıtları üzerinde sadece salt okunur yetkilere sahiptir. Sadece Süper_Yöneticiler kullanıcı hesaplarını düzenleyebilir ve TOE' nin kendi denetim verilerini görebilir.

TSF' in Korunması:

TOE ve TOE' nin çalışma ortamında bulunan tüm cihazlarla (veritabanı, arşiv sunucusu, vb.) kurmuş olduğu iletişim şifrelenmiş olarak yapılmalıdır. TOE hem kendiliğinden imzalı hem de kullanıcılar tarafından sağlanan sertifikaları desteklemelidir. Şifrelenmiş bir kanal kullanmak TOE' nin alt sistemleri/bileşenleri arasında özel ve güvenli bir iletişimi garanti eder. Herhangi bir verinin değiştirilmesi ya da herhangi bir veriye erişilmesi bu şifreli iletişimle engellenmiş olur.

TOE arşivi uygun bir karıştırma algoritması ile korunur. Alınan tüm denetim verileri TSF verilerinin bütünlüğünü sağlayabilmek amacıyla; önceden belirlenmiş bir zaman eşiğinden sonra bir arşivde tutulur, karıştırılır ve sıkıştırılır. Arşivlenmiş denetim verileri üzerinde yapılan herhangi bir değişiklik tekrar karıştırma ve elde edilen karıştırma değerleri karşılaştırılarak tespit edilebilir[FB1]. Zaman damgaları TSF verisinin bütünlük ve koruyuculuk yönünden izlenebilmesini sağlayan bir yöntemdir. Bu zaman damgaları harici olarak yetkilendirilmiş bir kurumdan alınabilir ya da TOE' nin işletim sitemi tarafından dâhili olarak uygulanabilir.

Sınıflandırılmış herhangi bir verinin/kaydın silinmesi ya da değiştirilmesi TOE tarafından engellenmiştir. Bu yüzden verilere ya da bu verilerin verilerine erişim kısıtlanmıştır.

Olay/Vaka Yönetimi:

TOE farklı ağ/güvenlik kaynaklarından denetim verileri/günlük kayıtları toplar. Günlük kayıtları toplanarak düzenlenir ve TOE üzerinde oluşturulmuş kurallara göre ilişkilendirilir. Yetkilendirilmiş kullanıcılar düzenlenmiş olay verilerine erişebilir ve bu verileri yapılandırmış oldukları kurallar vasıtasıyla ilişkilendirebilirler. TOE kullanıcıları alarmları tetikleyebilmek için eşik değerleri oluşturur. Tetiklenen olaylar GUI/CLI bilgi göndermek, önceden belirlenmiş adreslere e-posta göndermek veya komut/script çalıştırmak gibi işlemleri yapabilme kabiliyetine sahiptir.

TOE verilerin tutulduğu alanın/diskin/hafızanın boyutunu denetleyerek denetim/günlük kayıtlarının kaybolmamalarını garanti eder. Eğer denetim verilerine/günlük kayıtlarına ait alan önceden belirlenmiş bir eşik değerinin altına düşerse, yetkilendirilmiş kullanıcı e-posta ya da GUI/CLI aracılığıyla iletilen alarmla bilgilendirilir. Denetim verileri/günlük kayıtları gerekli alan açılana kadar verilerin kaynağı olan yerde tutulur veya belirli bir tarihten önce yer alan eski veriler, yeni verileri işlemek adına silinir.

High availability kontrol?[FB2]

İletişim:

TOE ve TOE' nin çalışma ortamında bulunan tüm cihazlarla (veritabanı, arşiv sunucusu, vb.) kurmuş olduğu iletişim şifrelenmiş olarak yapılmalıdır. Uygun bir şifreleme algoritması ve/veya sertifikalar bağlantıları güvenli kılmak için kullanılır. TOE hem kendiliğinden imzalı hem de kullanıcılar tarafından sağlanan sertifikaları desteklemelidir. Şifrelenmiş bir kanal kullanmak TOE' nin alt sistemleri/bileşenleri arasında özel ve güvenli bir iletişimi garanti eder. Herhangi bir verinin değiştirilmesi ya da erişilmesi bu şifreli iletişimle engellenmiş olur[FB3].

Hassas Verinin Karıştırılması/Şifrelenmesi:

TOE' ye ve/veya çevre birimlerine ait herhangi bir şifre ya da gizli veri hassas veri olarak değerlendirilir ve bu veriler düz metin olarak tutulmamalıdır; bu verilerin değiştirilme ya da kaybolma riskini azaltmak için veriler şifrelenmeli ya da karıştırılmalıdır. Şifrelenmiş ve/veya karıştırılmış veri üzerinde yapılabilecek herhangi bir tersine mühendislik yöntemini engelleyebilmek için yeteri kadar güçlü ve güvenli bir şifreleme ve/veya karıştırma algoritması seçilmelidir. Bu tür tehlikelerin risklerini azaltmak için TOE şifreleme ve/veya karıştırma algoritmalarını yeni algoritmalar geliştirildikçe güncellemelidir.

Kriptografik Destek:

TOE uygun ve güncel anahtar oluşturma algoritmaları sağlayarak ve uygun bir kriptografik anahtar sisteminden faydalanarak kriptografik anahtarlar oluşturur. Yeni bir anahtar oluşturulduğunda eski anahtarlar silinir/üzerine yazılır. Kullanıcı arayüzleri ve TOE' nin çevresiyle yaptığı tüm bağlantılar hassas bağlantılardır. Bu bağlantılar bahsi geçen şifreleme standartlarından faydalanılarak güven altına alınır.[FB4]

Yapılandırma Verilerinin Alınması/Gönderilmesi:

TOE' nin tüm yapılandırma ayarları olası bir yedekleme/geri alma durumuna karşı gönderilip alınabilmelidir. Yapılandırma verileri en azından aşağıdaki bilgileri içermelidir.

- TOE' nin tüm yapılandırma ayarları (IP ayarları, e-posta ayarları, vs.)
- Kullanıcı/Grup Kimlik Doğrulama/Yetkilendirme verileri (Kullanıcılar, gruplar ve izinler)

Otomatik Arşiv:

TOE yetkilendirilmiş kullanıcıların bir zaman eşiği tanımlayarak eski verilerin sunucudan gönderilmesini sağlayan bir arşivleme yöntemine sahiptir. Tanımlanmış bir tarihten eski veriler otomatik olarak arşivlenir, şifrelenir ve kaydedilir.

1.4. DOCUMENT OVERVIEW

In Section 1, TOE and Protection Profile are identified. With this introduction, security requirements and functions will be more easily understood.

In Section 2, conformance claims are explained. Conformance claims are Common Criteria conformance claim, Protection Profile conformance claim and EAL package conformance claim. Rationale of conformance claim and conformance statement defining type of the conformance are also explained in this chapter.

In Section 3, security problem definition is made and threats, assumptions and organizational security policies are listed to give an overall picture of the TOE with a security focus.

In Section 4, security objectives addressing threats, assumptions and organizational security policies explained in Section 3 will be explained and rationales are given accordingly.

In Section 5, extended components are defined and explained.

In Section 6, security requirements are explained in detail, making use of the components and assurance classes of Common Criteria Standard Part 2 and Part 3.

In the "References" section, some remarkable reference documents are referenced.

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE CLAIM

This protection profile conforms to the Common Criteria Standard, Version 3.1, Revision 4.

This protection profile is conformant to the Part 2 of the Common Criteria Standard, Version 3.1, Revision 4. Some extended components are included to fulfill the needs of analysis functionality. These are defined in Section 5, “Extended Components Definition”.

This protection profile is conformant to the Part 3 of the Common Criteria Standard, Version 3.1, Revision 4. All EAL4 level requirements are included as they are defined in Part 3 of the Standard. Evaluation Assurance Level is EAL4.

2.2. PP CLAIM

This protection profile doesn’t claim conformance to any other protection profiles.

2.3. EAL CONFORMANCE CLAIM

This protection profile is conformant to the Part 3 of the Common Criteria Standard, Version 3.1, Revision 4. All EAL4 level requirements are included as they are defined in Part 3 of the Standard. Evaluation Assurance Level is EAL4.

2.4. CONFORMANCE RATIONALE

This part is non-applicable, since it doesn’t claim any conformance to any other protection profiles.

2.5. CONFORMANCE STATEMENT

This protection profile requires “strict conformance”. Strict conformance requires that ST documents which will conform to this protection profile will need to fulfill all requirements defined in Section 6 of this protection profile.

3. SECURITY PROBLEM DEFINITION

3.1. OVERVIEW OF SECURITY PROBLEM DEFINITION

In this section, scope and form of the possible threats, organizational security policies and assumptions for the TOE, as well as related counter-measures (security objectives) are explained.

3.2. THREATS

In this section, threat agents and possible threats that can be caused by the agents are explained. Threats are divided into two categories, because there are two types of threats to the system; ones that aim protection of the TOE itself, others aiming a better analysis functionality for the TOE.

3.2.1. THREAT AGENTS

Bu bölüm içeriği EDRMS koruma profilinden alındı, ihtiyaç olursa değiştirilerek kullanılabilir.

Attacker	Attacker is the entity that is not an authorized user of the TOE... but uses his/her/its abilities to illegally become authorized. Attacker has a bad intent, motivation, system resources and time to cause damage on the TOE. The most dangerous kind of Attackers have advanced abilities and knowledge to cause damage. Another group of Attackers have limited ability and knowledge, but they are capable of using ready-to-use software tools to attack the TOE.
Normal_User	This threat agent doesn't have management role on the TOE. Normal_User is allowed to use some functions on the TOE. Normal_User uses the TOE functionality as a black box. Although it can be said that generally Normal_User doesn't have any malicious intent when using TOE, it can be otherwise as well. This threat agent can cooperate with the Attacker or can unintentionally fall into a trap of an Attacker.

3.2.2. THREATS

İLETİŞİMLE İLGİLİ TEHDİTLER (T.UNAUTHORIZED_ACCESS):

- TOE, diğer network cihazlarıyla ve sistem yöneticileriyle iletişim kurar. Bu cihazlar fiziksel veya sanal olarak ayrı konumda olabilir. Bu iletişim bir veya daha fazla sistem üzerinden gerçekleştiriliyor olabilir. Aradaki bu sistemler kötü niyetli kişilerce yönetiliyor olabilir. TOE, üç ayrı şekilde iletişim kurar: 1) Yine TOE'ye ait bir bileşenle kurulan iletişim, 2) TOE tarafından yönetilmeyen harici bir bileşenle kurulan iletişim, 3) Sistem yöneticileriyle kurulan iletişim. Bu üç iletişim şekli arasında alınacak önlemler açısından bir fark bulunmaz.
- TOE'ye yönelik önemli tehditlerden birisi, bahsi geçen iletişim kanalları üzerinden plaintext olarak aktarılan bilgilerdir. Örnek: şifreler, konfigürasyon ayarları, routing güncellemeleri. Bu bilgiler aradaki sistemler tarafından okunabilir veya değiştirilebilir. Bu durum ise TOE'nin ele geçirilmesiyle sonuçlanabilir.
- Güvenli iletişim için bazı protokoller tanımlanmıştır. Ancak bu protokollerin RFC tanımlarına uygun olduğu halde çok sayıda uygulanma opsiyonları vardır. Bu opsiyonlardan bazısı güvenlik açısından dezavantaj oluşturabilir.

- İletişim konusundaki başka bir tehdit, TOE ile iletişim kuran bileşenlerin, zararlı bir üçüncü tarafı TOE zannetmesinin sağlanması, veya TOE'nin zararlı üçüncü tarafı güvenilir zannetmesidir. Üçüncü taraf, iletişim taleplerini (requests) dinlemek ve sanki TOE imiş gibi talebe cevap vermek suretiyle bu tehditi ortaya çıkarır.
- Saldırgan, iletişimde aracı görevi gören bir sistemi ele geçirmek suretiyle de iletişimi dinleyebilir veya değiştirebilir.
- Güvenli bir protokol kullanılıyor olsa bile, gerekli güvenlik önlemleri alınmadığında saldırgan TOE'yi yanıltabilir. Örneğin yetkilendirme sürecindeki trafiği dinleyen saldırgan, bu trafiği "play back" yapmak suretiyle TOE'yi yanıltabilir.

GÜVENSİZ GÜNCELLEME TEHDİTLERİ (T.UNAUTHORIZED_UPDATE) :

- TOE'nin güncellenmesinde kulanılan prosedür yeterince güvenlik sağlamadığında, saldırgan kendi güncellemesini TOE'nin güncellemesi gibi gösterebilir.
- Bu tür tehditlere karşı alınabilecek önlem, güncellemelerin hash değerlerinin alınması, hatta bu hash değerleri üzerinde kriptografik işlemler gerçekleştirilmesidir (örneğin güvenli elektronik imza).
- Zayıf güvenlikli bir hash fonksiyonu kullanıldığında, saldırgan hash değerini değiştirmeden güncellemeyi modifiye edebilir.
- Kök sertifikası ele geçirildiyse, güçlü bir hash algoritması kullanılsa bile zararlı bir güncellemenin yapılmasına engel olunamaz.

TESPİT EDİLEMEYEN OLAY KAYITLARI (T.ADMIN_ERROR, T.UNDETECTED_ACTIONS, T.UNAUTHORIZED_ACCESS) :

- Sistem yöneticisi farkında olmadan güvenlik konfigürasyonunu hatalı ayarlayabilir. Böylece güvenlik olayları kaydedilmeyebilir veya takip edilemeyebilir.
- Bu koruma profilinde TOE'nin audit verilerini tutacağı belirtilmişse de, TOE'nin bunları kendisi tutması zorunluluğu yoktur. TOE bu kayıtları başka bir bileşene (örneğin syslog server) gönderir. Bu bileşenle aradaki iletişim kanalları yeterince güvenli değilse, saldırgan gönderilen kayıtları modifiye edebilir. Başka bir tehdit ise, bu harici bileşene erişilememesidir.

TOE'YE ERİŞİM (T.UNAUTHORIZED_ACCESS) :

- Yetki verilmiş hesaplardan birisi ele geçirilmiş olabilir. Bunun en birincil sebebi, zayıf şifrelerin kullanılmasıdır. Kısa şifreler, şifrelerde sözlük kelimelerinin kullanımı, uzun süre aynı şifrenin kullanılması gibi durumlar bu tehdite ortam hazırlar. Şifre girildiği an görülebilir durumdaysa, yine tehdit oluşabilir.
- Şifre değiştirme anında şifreyi değiştiren kişinin yetkili kişi olduğundan emin olunmazsa, herhangi bir kişi bir hesabı ele geçirebilir.
- Yetkilendirilmiş bir kişi, bir süre için cihazın başından ayrıldığında başka birisi hesabı kullanmaya devam edebilir.

KULLANICI VERİSİNİN YENİDEN KULLANILMASI (T.USER_DATA_REUSE) :

- TOE içerisinde dolaşan veri istenmeden farklı bir kullanıcıya gönderilebilir. Bunu tam anlamadım.

TSF HATASI (T.TSF_FAILURE) :

- TOE üzerindeki güvenlik mekanizmaları genellikle basit mekanizmaların birbirine eklenerek karmaşık mekanizmalar oluşturması ile sağlanır. Basit mekanizmalarda (örneğin memory yönetimi, process önceliklendirmesi gibi) meydana gelen güvenlik açıkları daha karmaşık mekanizmalarda da güvenlik açığı oluşmasına sebep olabilir.

T.UNAUTHORIZED_ACCESS	• Harici bileşenlerle veya Administrator ile iletişim kurarken bilgi sızabilir. ○ Örneğin denetim verisinin toplandığı cihazlarla aradaki iletişim kötüye kullanılabilir. • Veri aktarımı için kullanılan güvenlik protokollerinin konfigürasyonları iyi yapılmamış olabilir.

	● Aradaki kişi iletişim taleplerini dinler ve sanki muhatap kendisiymiş gibi karşı tarafa cevap verir. ● Trafiği dinleyen bir saldırgan, daha sonra bu trafiği "play back" yapabilir. ● Yetki verilmiş hesaplardan birisi ele geçirilmiş olabilir. ● Saldırgan şifrelerin saklandığı kayıtları inceleyerek şifreleri ele geçirebilir. ● Şifre değiştirme anında şifreyi değiştiren kişi aslında yetkisiz bir kişi olabilir. ● Uzun süre aynı şifrenin kullanılması da şifrenin ele geçirilmesi ihtimalini artırır. ● Şifrenin girilmesi anında kişi gözlenerek şifre öğrenilebilir. ● Yetkilendirilmiş bir kişi cihazın başından ayrıldığında, yetkisiz kişi hesaba erişim sağlayabilir.
T.UNAUTHORIZED_UPDATE	● Saldırgan kendi güncellemesini TOE'nin güncellemesi gibi yükletebilir. ● Hash değerinin ve yüklemenin bulunduğu sistem ele geçirilirse, saldırgan hem hash değerini hem de güncellemeyi değiştirebilir. ● Kök sertifikasını ele geçiren bir saldırgan, kuvvetli hash fonksiyonu kullanılsa bile zararlı güncellemeyi kurabilir.
T.REPUDIATION	● Yetkilendirilmiş veya yetkilendirilmemiş kullanıcılar, TOE üzerinde gerçekleştirdikleri işlemleri inkar edebilir. ● Sistem yöneticisi, yanlışlıkla denetim kayıtlarının yanlış bir şekilde tutulacağı veya tutulmayacağı bir konfigürasyon belirlemiş olabilir. ● TOE, denetim kayıtlarının tutulması için üçüncü bir tarafa güveniyor olabilir. Ancak bu üçüncü tarafa erişilememesi söz konusu olabilir. ● Üçüncü tarafla iletişim güvenilir olmadığında, gönderilen kayıtlar modifiye edilebilir.
T.MALICIOUS_IMPORT	● Her ne kadar TOE denetim verilerini topladığı esnada dosya bütünlüğünü ve dosyanın kaynağını tespit ediyorsa da, verilerin elde edildiği üçüncü tarafların zararlı kişilerce ele geçirilmiş olması ihtimali söz konusudur.
T.USER_DATA_REUSE	● Saldırgan, TOE bünyesinde kalmış herhangi bir kullanıcıya ait verileri kullanarak sisteme sızmak için veri elde edebilir.
T.MISCONFIGURATION	● TOE hatalı bir şekilde konfigüre edilmiş olabilir.
T.TSF_FAILURE	● TOE, dosya sistemindeki alanın yetersizliği, hızlı bellek yetersizliği, denetim kayıtlarını tutan birime ulaşamama, vb. sebeplerden ötürü çalışması aksayabilir.
T.DATA_DISCLOSURE	● Yetkisiz bir kişi TSF verisini aşikar edebilir.
T.DATA_MODIFICATION	● Yetkisiz bir kişi TOE tarafından analiz edilen verileri ve analiz sonrasında ortaya çıkan verileri değiştirebilir veya silebilir.
T.DENIAL_OF_SERVICE	● Yetkisiz bir kullanıcı TOE'yi kapatabilir veya çok fazla veri göndererek TOE'nin bunları işleyemez hale gelmesini sağlayabilir.
T.FAILED_RECOGNITION	TOE, veri kaynaklarından elde edilen bilgileri kullanarak gerçekleştirdiği analizlerde zafiyetleri ve anormal davranışları tespit edemeyebilir.
T.FAILED_ACTION	TOE, belirlenmiş veya şüphe duyulan güvenlik olaylarına karşı önlem almayabilir veya önlem almakta gecikebilir. Alınan önlem, güvenlik olayına karşı etkili olmayacak bir önlem olabilir.
T.FAILED_ASSOCIATION	TOE, ilişkileri tespit edilmiş olan denetim verilerinden faydalanarak gerçekleştirdiği analizlerde zafiyetleri ve anormal davranışları tespit edemeyebilir.

T.UNAUTHORIZED_ACCESS	Attacker can make an attempt to get access to TOE by using a fake/stolen identity. This attempt can be made by using a stolen identity, a faked IP address, etc. The Attacker can get unauthorized access to the TOE by making use of security breaches like keeping default usernames and passwords unchanged, use of simple passwords, not disabling test accounts on real system, unsatisfactorily controlled uploading feature. Besides, the Attacker can benefit from residual data of a previous or an active user or residual data that is created during internal or external TOE operation and communication. These data can be a critical data about the users of the TOE or the TOE itself. Attacker can have access to these data and can ease his/her/its access to the TOE, cause damage depending on the content of the data. Attacker can also access confidential data used for authentication by misguiding System_Administrator, Data_Entry_Operator or Normal_User. For instance, Attacker can have access to confidential data by redirecting System_Administrator, Data_Entry_Operator or Normal_User to a web address which doesn't belong to TOE and make the users believe that they are protected by the TOE.
T.DATA_ALTERATION	Records, documents and data protected by the TOE can be modified without permission. The Attacker can misguide System_Administrator, Data_Entry_Operator or Normal_User, to obtain TSF data or data of a specific user. The Attacker can also authorize itself illegally and change records, documents and/or other data protected by the TOE. This threat generally occurs when the integrity of the records and documents is not assured. The Attacker can also try to alter audit data. This threat occur when integrity of audit data is not assured. Another occurence of this threat is modification of the source codes and audit data of the TOE by the Attacker. Inproper file permissions or insufficient control of incoming data/files may be the cause of this threat. The Attacker may get unauthorized access to the TOE by benefiting from this threat.
T.REPUDIATION	An action or a transaction (a queue of actions) made on the TOE can be repudiated. It is relatively easier to repudiate actions on the TOE when insufficient or inproper audit mechanisms exist. It is usually the last task of the Attacker on the TOE, to make sure that the System_Administrator doesn't become aware of the attacking and so doesn't have the ability to take the needed actions. Additionally the Attacker can prevent audit records to be in place (for instance, by causing an overflow in audit trail). Or the Attacker can add false / high number of records to audit trail to mislead the System_Administrator.
T.DATA_DISCLOSURE	Confidential data protected by the TOE can be disclosed without permission. For instance, Normal_User can access to a record, document or data, thathe/she is unauthorized to access. Insufficient parameter controls may cause this threat. A Normal_User or Data_Entry_Operator can intentionally or unintentionally disclose confidential information by using the functinality offered by the TOE. For instance, existence of confidential user data on statistical reports is a kind

	of this threat. Showing credit card information of any user along with other information in user details interface is another kind of this threat. Yet another kind of this threat is that allowing bulk export /view of user data or TSF data using TOE functionality to the users having limited privileges. Another occurence of this threat is the possibility of an Attacker to disclose TSF data by using his/her attack potential.
T.DENIAL_OF_SERVICE	The Attacker can cause the TOE to become unavailable or unusable for a period of time. This is usually done by sending too many requests in a small period of time that the TOE becomes unable to respond. Simple type of denial of service includes sending too many request from a specific IP range. This is called Denial of Service (DoS). A more advanced type of denial of service threat is Distributed Denial of Service (DDoS). For DDoS attacks, no specific IP range is used. Usually BOTNETs are used for DDoS attacks. Since there is not a restriction on incoming IP addresses, it is either hard or too expensive to distinguish between normal and malicious requests.
T.HARMFUL_DATA	The Attacker can import a harmful record, document or data into the TOE. By using this threat, the Attacker can have access the data of a specific user, can take over the account of a user or can access to a part or the whole of the TOE functionality. It is a quite common fact that when the Attacker gains access, he/she/it tries to form new ways (back doors) to access to the TOE by changing TSF parameters or parameters in working environment, by defining a new user account, opening an alternative port, etc. Even when the cause of the threat is cured, the Attacker may continue to access to the TOE using the back door.
T.ELEVATION_OF_PRIVILEGES	The Attacker can gain limited access to the TOE by benefiting from the threats like T.UNAUTHORIZED_ACCESS, T.HARMFUL_DATA and T.DATA_ALTERATION, and then try to gain a higher level of privilege, or a Normal_User can try to gain higher level of privilege by using his/her existing privileges. This threat is usually caused by the fact that interfaces for authorized users are not secured as strong as the interfaces not requiring an authorization.

3.3. ORGANIZATIONAL SECURITY POLICIES

P.REGULATIONS	İçişleri Bakanlığı tarafından yayınlanan tebliğ. 5651 sayılı kanunun loglarla ilgili hükümleri 5070 sayılı kanun da buraya yazılabilir mi? **Aşağıdaki OSP'ler EDRMS koruma profilinden alındı. İhtiyaç olursa kullanılabilir.**
P.PROPER_CONFIGURATION	Default configuration of the TOE and interacting components that are under the control of the TOE shall be changed, so that the Attacker can't get information about the TOE and its operational environment. Unused services shall be deactivated. Configuration parameters include (but not limited to) default root directories, default error and 404 pages, default authentication values, default usernames, default ports, default pages that reveal internal information like configuration settings, version number, etc. Although all conformant products shall fulfill this requirement, this organizational security policy is especially important when the TOE or any

	interacting component is a widely used product. By ensuring unique configuration parameters, the Attacker can be prevented from attacking by using the information gained by a similar IT product.
P.E_SIGNATURE	e-Signatures that are used for electronically signing operations shall be conformant to Turkish Electronic Signature Law numbered 5070. Accordingly, signing procedures shall follow the same law.
P.ACCOUNTABLE	Users of the TOE shall be accountable for their actions within the TOE.

3.4. ASSUMPTIONS

A.TRUSTED_ADMIN	It is assumed that all users responsible for installation, configuration and management of the TOE are sufficiently qualified and educated, and they are following the rules properly.
A.TRUSTED_DEVELOPER	It is assumed that people responsible for the development of the TOE (like coder, designer, etc.) are trusted entities and they follow the rules properly without any malicious intentions.
A.EXPERIENCED_DEVELOPER	It is assumed that all users developing the TOE are experienced in the field of security and they take all the needed counter-measures for all known security vulnerabilities.
A.AVAILABILITY	It is assumed that the TOE has access to all the IT System data it needs to perform its functions.
A.SCALABILITY	It is assumed that the TOE is appropriately scalable to the IT System the TOE monitors and data payload that it is meant to collect, analyze and correlate.
A.SECURE_ENVIRONMENT	It is assumed that needed physical and environmental precautions has been taken for the working environment of the TOE. It is also assumed that access to the working environment of the TOE is properly restricted and access records are kept for a reasonable amount of time.
A.PROPER_BACKUP	It is assumed that any data created or imported by the TOE, storage unit(s) and other hardware components have proper backups, so that no data loss or service interruption occurs because of a system failure. With respect to workflow of the TOE, the most important environmental component is the storage in which audit records are being kept.
A.EXT_COMMUNICATION	It is assumed that all communication and communication channels used by the TSF to communicate external entities, which are not under the protection of TSF, are sufficiently secured.
A.SECURE_DELIVERY	It is assumed that all needed security measures have been taken during the delivery of the TOE. Delivery processes have been caried out by qualified and

	trusted entities.
A.SECURE_AUDIT_LOGS	It is assumed that all audit logs which will be accepted by the TOE are secure and don't contain harmful content.

4. SECURITY OBJECTIVES

4.1. INTRODUCTION

In this section, security objectives for the TOE and its working environment are explained.

Security objectives are separated into two parts as security objectives for the TOE and security objectives for the operational environment. Security objectives for the TOE are addressed by the TSF, others are not. These security objectives define the requirements that the TOE and/or its operational environment should meet. These objectives will be mapped to security functional requirements in Section 6.

4.2. SECURITY OBJECTIVES FOR THE TOE

O.AUDIT	TOE shall record any event having value in terms of security within the scope of its ownership. TOE shall protect these records against modification and deletion. TOE shall provide explicitly authorized users the functionality to review the records easily and quickly, making it possible for System_Administrator to be timely informed about critical security events.
O.AUTH	TOE shall explicitly define every user, securely authenticate them and authorize them according to their rights and roles. All requests needing authorization shall be subject to authentication and authorization processes. The TOE shall define the rules for user authentication that forces users to have strong passwords. TOE shall allow classification of records/documents, provide the functionality to define rules with respect to record/document classification. TOE shall also offer the ability to define rights for individual records/documents. TOE shall provide a record/document level access control mechanism to individual users or groups of users. An Attacker can try to benefit from T.ELEVATION_OF_PRIVILEGE threat. To help prevent this threat, TOE shall authenticate the System_Administrator using stronger mechanisms. Examples of such mechanisms are IP-range restriction, time-period restriction, token-based authentication, multi-factor authentication, a combination of these, etc. Third party tools used by the TOE shall be configured to run at minimum authorization level possible. Default parameters of these tools shall be modified, so that they become unique and aren't affected by automatized attacks.
O.DATA_FLOW_CONTROL	TOE shall control and manage unauthorized data flow in and/or out. Data to be imported shall be subject to content filtering. A high number of requests from a definite IP range can be a signal of denial of service attack. The TOE shall provide the System_Administrator with an easily usable interface to let him/her keep the network traffic under observation and let the System_Administrator put filtering mechanisms in place if needed.

	Additionally, TOE shall take precautions against viewing, exporting, modifying and deleting TSF or user data without a reasonable aim, even if these operations are carried out by using the functions provided by the TOE itself.
O.DATA_INTEGRITY	TOE shall ensure data integrity for audit data and record data by detecting any modification on these data, takes needed actions when any modification occurs.
O.MANAGEMENT	TOE shall provide the System_Administrator with all the functionality to manage the system securely and effectively. TOE shall put proper access control mechanisms in place to protect management interfaces. TOE shall also ensure that its interfaces support fast and accurate decision making. TOE shall provide the System_Administrator with the ability to change rights and roles of the users, and can explicitly set rights and roles for a specific user and/or group. System_Administrator shall give the users rights and roles according to “need to know” basis.This security objective also ensures that proper protection mechanisms against Denial of Service are taken.
O.ERROR_MANAGEMENT	TOE shall offer an error management mechanism in a secure and efficient way. Errors occuring during the operation of the TOE shall be shown to the user in a secure and meaningful way. For instance, TOE shall return a general authentication failure information, not a specific one like “username is not found”. Similarly, error details with method and line of code shall not be exposed to normal users. On the other hand, System_Administrator shall be informed about critical failures in a fast and efficient way. Errors shall be detailed enough to lead the System_Administrator to suitable actions. The TOE shall preserve a secure state in case of an error occuring in the TOE itself.
O.RESIDUAL_DATA_MNG	TOE shall ensure that any residual data is removed from the TOE or made inaccessible to users when it is no longer needed.

4.3. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.SECURE_ENVIRONMENT	Operational environment of the TOE shall ensure physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components. Operational environment of the TOE shall ensure that the TOE is properly protected against any denial of service or distributed denial of service attacks. Possible protection mechanisms include, but not limited to: ● Deactivation of unused services, ports, etc. ● Creation of IDS and IPS signatures ● Shorter period of DNS timeout ● A policy to ensure additional bandwidth to be in place in a short period of time ● Static web page copies ● IP address blocking and black listing ● Activation of DoS protection modules that exist in web server

- Using reverse proxy

OE.COMMUNICATION	Operational environment of the TOE shall provide the TOE with secure communication mediums and/or tools.
OE.TRUSTED_ADMIN	Operational environment of the TOE shall ensure that all users using the management functions of the TOE are sufficiently educated and meet the security requirements.
OE.TRUSTED_DEVELOPER	Operational environment of the TOE shall ensure that all users developing the TOE are sufficiently educated and meet the security requirements.
OE.EXPERIENCED_DEVELOPER	Operational environment of the TOE shall ensure that all users developing the TOE are experienced in the field of security and they take all the needed counter-measures for all known security vulnerabilities.
OE.COMPLEMENTARY_AUDIT	Operational environment of the TOE shall ensure that any security related event for the components other than the TOE itself is subject to audit operations. This operational environment security objective complements O.AUDIT security objective and does its job on the operational environment of the TOE. Audit records for the TOE are more meaningful if they are combined with the remaining audit records. Hence, all audit records shall be easily monitored with minimal workload.
OE.SECURE_DELIVERY	Delivery and installation of the TOE shall be carried out without sacrificing any security constraint. Besides, functions and/or parameters used for testing purposes shall be cleared or made inaccessible.
OE.PROPER_BACKUP	Proper backups shall be created and kept for a reasonable time for all data residing in the operational environment of the TOE. Pre-defined routines may be used for this purpose. Storage units and other hardware components shall also be backed up for the TOE to be reliable enough.

4.4. SECURITY OBJECTIVES RATIONALE

Security objectives rationale verifies that identified security objectives are necessary, suitable and sufficient for addressing security problems.

These points have been verified by security objectives rationale:

- At least one security objective is defined for each threat, organizational security policy and/or assumption.
- Each security objective is addressing at least one threat, organizational security policy and/or assumption.

Please refer to Table 1 for a general overview.

4.4.1. RATIONALE OVERVIEW

Table 1 shows the relation between security objectives and security problem definition elements (threats, OSPs and assumptions). Threats are generally addressed by security objectives for the TOE, whereas OSPs and assumptions are addressed by security objectives for the operational environment of the TOE.

Table 1: Relation Between Security Problem Definition and Security Objectives

4.4.2. RATIONALE FOR THE TOE

O.AUDIT	O.AUDIT security objective offers an audit mechanism. This mechanism helps the System_Administrator to identify any repudiation attempt by ensuring audit records to be kept and by providing integrity of the records. This security objective addresses **T.REPUDIATION** threat. This security objective is also strongly related with **P.COMPLEMENTARY_AUDIT**, since audit mechanism of the TOE and audit mechanism of the operational environment are helping each other to solve security issues.
O.AUTH	This security objective ensures a proper authentication and authorization mechanism and therefore it is directly addressing **T.UNAUTHORIZED_ACCESS**. Besides, a strong authentication and authorization mechanism prevents data alteration. Since it is ensured that System_Administrator is subject to more advanced authentication mechanisms, this security objective is also addressing elevation of privilege threat. Therefore, this security objective addresses **T.ELEVATION_OF_PRIVILEGE**. This security objective is also in relationship with **T.DATA_ALTERATION**, since it ensures the integrity of the audit records. This security objective is also related with **T.DATA_DISCLOSURE**, since a good authentication mechanism is a means of data disclosure prevention. It is also related with **P.RECORD_VERIFICATION** OSP, since record verification policy introduces some measures for authentication.
O.DATA_FLOW_CONTROL	This security objective secures the communication channels and defines data control principles. Hence, it addresses **T.HARMFUL_DATA**. Since this objective tries to manage data flow, it can also detect unusual number of data flow or data requests from a specific IP range. Hence, it addresses **T.DENIAL_OF_SERVICE** threat. This security objective can prevent unauthorized access by allowing authentication data to be securely sent. It also prevents data alteration and data disclosure during transmission. This security objective addresses **T.DATA_ALTERATION** and **T.DATA_DISCLOSURE** threats as well. Besides, it is addressing **P.SSL_COMMUNICATION**, since this OSP has some restrictions on communication channels. **P.PROPER_CONFIGURATION** can also be related with this security objective, since configuration parameters help prevent unauthorized data flow. It is also related with **P.RECORD_VERIFICATION** OSP, since record verification policy introduces some measures against information disclosure.
O.DATA_INTEGRITY	This security objective ensures that the TOE is able to detect and take needed actions against any data modification on audit data and record data. This security objective addresses **T.DATA_ALTERATION** threat. Additionally, since usage of e-signatures is included in data integrity operations, this security objective also addresses **P.E_SIGNATURE** OSP.
O.MANAGEMENT	This security objective provides the System_Administrator with all needed management functions to securely manage the TOE. Provided management functions addresses issues related with authentication, authorization and data disclosure. Hence, this security objective addresses **T.UNAUTHORIZED_ACCESS**,

	T.DATA_DISCLOSURE and **T.ELEVATION_OF_PRIVILEGE**. Access Control Policy defined in management functions provide mechanisms to take needed measures against denial of service attacks. Hence, this objective addresses **T.DENIAL_OF_SERVICE** threat as well. This security objective is also related with **P.PROPER_CONFIGURATION**, since configuration management is a branch of TOE management.
O.ERROR_MANAGEMENT	This security objective supports the TOE with error management functionality. Content of error messages can be used for elevation of privilege. Hence, this security objective addresses **T.ELEVATION_OF_PRIVILEGE** threat. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration helps for a better error management.
O.RESIDUAL_DATA_MNG	This security objective manages the residual data existing on the TOE. Residual data can be used for unauthorized access and elevation of privilege. It is also a kind of data disclosure. Hence, this security objective addresses **T.UNAUTHORIZED_ACCESS** and **T.ELEVATION_OF_PRIVILEGE** threats.

4.4.3. RATIONALE FOR THE OPERATIONAL ENVIRONMENT

OE.SECURE_ENVIRONMENT	This security objective for the operational environment is directly addressing **A.SECURE_ENVIRONMENT** assumption. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration is a core component of a secure environment. This security objective for the operational environment also addresses **T.DATA_DISCLOSURE** and **T.DENIAL_OF_SERVICE** threats, since both threats need additional measures which are need to be taken by the operational environment of the TOE. Since proper protection against distributed denial of service attacks need precautions for operational environment, this security objective for operational environment is addressing **A.DIST_DENIAL_OF_SERVICE** assumption.
OE.TRUSTED_ADMIN	This security objective for the operational environment is directly addressing **A.TRUSTED_ADMIN** assumption.
OE.TRUSTED_DEVELOPER	This security objective for the operational environment is directly addressing **A.TRUSTED_DEVELOPER** assumption.
OE.EXPERIENCED_DEVELOPER	This security objective for the operational environment is directly addressing **A.EXPERIENCED_DEVELOPER** assumption. Besides, this security objective also addresses **T.UNAUTHORIZED_ACCESS** and **T.DATA_DISCLOSURE** threats, since an experienced developer is the only means for a high-level security in terms of access control and data protection.
OE.COMPLEMENTARY_AUDIT	This security objective for the operational environment is directly addressing **P.COMPLEMENTARY_AUDIT** organizational security policy. Since this security objective is mapped to an organizational security policy, it is evidence based. In other words, it should be proven that proper audit mechanisms exist for the operational environment of the TOE.
OE.COMMUNICATION	This security objective for the operational environment is directly addressing **A.COMMUNICATION** assumption. This security objective is also related with **P.SSL_COMMUNICATION**. Although P.SSL_COMMUNICATION is meant to secure communication channels under the control of the TSF, it has a positive impact on

	the security of communication channels of the operational environment. Because TOE owns / is part of some of communication channels. This security objective is also related with **P.E_SIGNATURE**, since e-signature helps some degree of reliability to the communication.
OE.PROPER_BACKUP	This security objective for the operational environment is directly addressing **A.PROPER_BACKUP** assumption.
OE.SECURE_DELIVERY	This security objective for the operational environment is directly addressing **A.SECURE_DELIVERY** assumption. This security objective is also related with **P.PROPER_CONFIGURATION**, since a proper configuration helps for the secure delivery of the TOE.

5. EXTENDED COMPONENTS DEFINITION

This protection profile does not require any extended security functional components or security assurance components.

6. SECURITY REQUIREMENTS

6.1. SECURITY FUNCTIONAL REQUIREMENTS

6.1.1. USED NOTATIONS

This section explains needed security functional requirements. Rewritten parts to the component definition are shown as bold text. Unchanged content are shown intact.

Notations used in this section are as follows:

“Application Note” is added when there is a need to clarify possible misunderstanding about the application of component requirements. Besides, “PP Author Note” is added when it is needed to give extra information to ST Author or to make further restrictions on the components.

After every component definition, rationale of the component has been given to improve readability.

There are some allowed operations in protection profiles, which are defined in reference documents of Common Criteria Standard. A brief explanation about the operations are explained below. For further information please refer to the reference documents.

Refinement operation (denoted in such a way that added words are in **bold text** and changed words are ~~crossed-out~~): is used to add details to a requirement, and thus further restricts a requirement.

Selection operation (denoted by **bold text** starting with “selection:” and placed in square bracket): is used to select one or more options provided by the [CC] in stating a requirement.

Assignment operation (denoted by **bold text** starting with “assignment:” and placed in square bracket): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.

Iteration operation are identified with a number in round bracket (e.g. (1) , (2))

When editing security functional components, bold assignments are filled out by PP author. Those are not meant to be changed by ST author. But there are some assignments that is left to ST author. These assignments may be changed by ST author. These fields are not made bold to distinguish between remaining assignments.

6.1.2. OVERVIEW

Components included in this Protection Profile are shown in Table 2.

Table 2: List of Included Security Functional Components

Component Code	Component Name
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FAU_SAA.4	Complex attack heuristics

FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.2	Guarantees of audit data availability
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cyrptographic key generation
FCS_CKM.4	Cyrptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based 29ccess control
FDP_DAU.1	Basic data authentication
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.2	Full residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPR_UNO.4	Authorised user observability
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RCV.4	Function recovery
FPT_STM.1	Reliable timestamps
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
FTA_SSL.1	TSF initiated session locking
FTA_SSL.4	User-initiated termination
FTA_TAH.1	TOE access history
FTA_TSE.1	TOE session establishment
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

6.1.3. SECURITY FUNCTIONAL POLICIES

Access Control Policy

Access Control Policy is a policy that defines actions and restrictions about access to information protected by the TOE. Details about this policy can be found in the definitions of the components FDP_ACC.1 and FDP_ACF.1.

6.1.4. CLASS FAU: SECURITY AUDIT

FAU_ARP.1	**Security alarms**
Hierarchical to:	No other components.
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1:	The TSF shall take [assignment: list of actions] upon detection of a potential security violation.

Application Note: Examples of actions to be taken are deactivating some ports, changing configuration parameters, blocking IP addresses or IP-ranges, etc. But no strict definitions have been made for this component, since some external components don't have the capability to allow proper actions. At least, TSF shall inform the System_Administrator about the security violation. Provided that external component has the needed capability, the TSF shall use the capability for further actions instead of just informing System_Administrator.

FAU_GEN.1	**Audit data generation**
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1:	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[selection: basic (These events are listed in Table 3 below)]** level of audit; and c) [assignment: other specifically defined auditable events]
FAU_GEN.1.2:	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: other audit relevant information]**.

Application Note: System_Administrator shall have the possibility to choose among auditable event groups/types. Since this capability requires that auditable events can be selected dynamically, any change in the list of auditable events shall be auditable as well and marked as "critical". Results of the auditable events can be a one digit indicating success/failure or can be a wider range, according to the auditing procedure provided by the TOE. On the other hand, success or failure of events shall be easily observable and automatically sortable/filterable/groupable.

> ***Rationale:*** *This component is the main component defining the auditing requirements of the TOE. This component makes contribution to O.AUDIT security objective.*

Table 3: List of Auditable Events

Component	Auditable Event	Details
FAU_ARP.1	(minimal) Actions taken due to potential security violations.	
FAU_SAA.1	(minimal) Enabling and disabling of any of the analysis mechanisms; (minimal) Automated responses performed by the tool.	
FAU_SAA.4	(minimal) Enabling and disabling of any of the analysis mechanisms; (minimal) Automated responses performed by the tool.	
FAU_SAR.1	(basic) Reading of information from the audit records.	
FAU_SAR.2	(basic) Unsuccessful attempts to read information from the audit records.	
FAU_SAR.3	(detailed) the parameters used for the viewing.	
FAU_STG.3	(basic) Actions taken due to exceeding of a threshold.	
FAU_STG.4	(basic) Actions taken due to the audit storage failure.	
FCS_CKM.1	(minimal) Success and failure of the activity. (basic) The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM.4	(minimal) Success and failure of the activity. (basic) The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_COP.1	(minimal) Success and failure, and the type of cryptographic operation. (basic) Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FDP_ACF.1	(minimal) Successful requests to perform an operation on an object covered by the SFP. (basic) All requests (successful and unsuccessful) to perform an operation on an object covered by the SFP. (detailed) The specific security attributes used in making an access check.	Identification data of the object.
FDP_DAU.1	(minimal) Successful generation of validity evidence. (basic) Unsuccessful generation of validity evidence. (detailed) The identity of the subject that requested the evidence.	
FDP_IFF.1	(minimal) Decisions to permit requested information flows. (basic) All decisions on requests for information flow. (detailed) The specific security attributes used in making an information flow enforcement decision. (detailed) Some specific subsets of the information that has flowed based upon policy goals (e.g. auditing of downgraded material).	
FIA_AFL.1	(minimal) The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	
FIA_SOS.1	(minimal) Rejection by the TSF of any tested secret; (basic) Rejection or acceptance by the TSF of any tested secret.	For example, rejection or acceptance of user

	(detailed) Identification of any changes to the defined quality metrics.	password.
FIA_UAU.2	(minimal) Unsuccessful use of the authentication mechanism; (basic) All use of the authentication mechanism.	
FIA_UID.2	(minimal) Unsuccessful use of the user identification mechanism, including the user identity provided; (basic) All use of the user identification mechanism, including the user identity provided.	Provided user identity, source of attempt (identity of connected endpoint, source address, etc.)
FMT_MOF.1	(basic) All modifications in the behaviour of the functions in the TSF.	
FMT_MSA.1	(basic) All modifications of the values of security attributes.	
FMT_MSA.3	(basic) Modifications of the default setting of permissive or restrictive rules. (basic) All modifications of the initial values of security attributes.	
FMT_SMF.1	(minimal) Use of the management functions.	
FMT_SMR.1	(minimal) Modifications to the group of users that are part of a role; (detailed) every use of the rights of a role.	
FPR_UNO.4	(minimal) The observation of the use of a resource or service by a user or subject.	
FPT_RCV.4	(minimal) if possible, the impossibility to return to a secure state after a failure of the TSF; (basic) if possible, the detection of a failure of a function.	
FPT_STM.1	(minimal) changes to the time; (detailed) providing a timestamp.	
FTA_MCS.2	(minimal) Rejection of a new session based on the limitation of multiple concurrent sessions. (detailed) Capture of the number of currently concurrent user sessions and the user security attribute(s).	
FTA_SSL.1	(minimal) Locking of an interactive session by the session locking mechanism. (minimal) Successful unlocking of an interactive session. (basic) Any attempts at unlocking an interactive session.	
FTA_SSL.4	(minimal) Termination of an interactive session by the user.	
FTA_TSE.1	(minimal) Denial of a session establishment due to the session establishment mechanism. (basic) All attempts at establishment of a user session.	
FTP_ITC.1	(minimal) Failure of the trusted channel functions. (minimal) Identification of the initiator and target of failed trusted channel functions. (basic) All attempted uses of the trusted channel functions. (basic) Identification of the initiator and target of all trusted channel functions.	
FTP_TRP.1	(minimal) Failures of the trusted path functions. (minimal) Identification of the user associated with all trusted path	

	failures, if available. (basic) All attempted uses of the trusted path functions. (basic) Identification of the user associated with all trusted path invocations, if available.	

FAU_GEN.2	**User identity association**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_GEN.2.1:	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Rationale: *This component associates the audit records of the TOE with the users of the TOE. This component makes contribution to O.AUDIT security objective.*

FAU_SAA.1	**Potential violation analysis**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAA.1.1:	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2:	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: subset of defined auditable events] known to indicate a potential security violation; b) [assignment: any other rules]

FAU_SAA.4	**Complex attack heuristics**
Hierarchical to:	No other components.
Dependencies:	No dependencies
FAU_SAA.4.1:	The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios [assignment: list of sequences of system events whose occurrence are representative of known penetration scenarios] and the following signature events [assignment: a subset of system events] that may indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.4.2:	The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of **[assignment: audit records collected from various external entities, along with internal audit records]**.
FAU_SAA.4.3:	The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system activity is found to match a signature event or event sequence that indicates a potential violation of the enforcement of the SFRs.

Application Note: For this component to work effectively, TOE shall maintain a list of known sequences of system events whose occurence are representative of known penetration scenarios. This list shall be protected from unauthorized deletion or modification. Although this component may use the output of an Intrusion Detection System (IDS), it is not identical with it. “Signature events” mean any sequence of events, which are known as a strong signal of an intrusion.

PP Author Note: There is no need to list all sequences of system events in Security Target documents, an explanation of how they are kept is enough.

FAU_SAR.1	**Audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1:	The TSF shall provide **[assignment: users belonging to the roles, which grants at least read access to audit trail]** with the capability to read **[assignment: all audit information]** from the audit records.
FAU_SAR.1.2:	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Rationale: *This component provides the users of the TOE with a human-readable interface to the audit records. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

FAU_SAR.2	**Restricted audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1:	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application Note: Application level access prohibition is aimed with this component. It is assumed that access restriction mechanisms for operating system and storage unit(s) are provided by external entities.

Rationale: *This component restricts audit reviewing functionality to explicitly authorized users. This feature contributes to audit and management of the TOE. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

FAU_SAR.3	**Selectable audit review**
Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.3.1:	The TSF shall provide the ability to apply **[assignment: filtering and sorting]** of audit data based on **[assignment: filtering parameters; risk rating, time period, source IP address, destination IP address and** [assignment: other filtering parameters] **and sorting parameters; event ID, event type, time, signature ID (optional), SIEM actions performed (optional),** [assignment: other sorting parameters]**]**.

Rationale: *This components introduces an ability to TOE, with which audit records can be shown to the user in a selectable format. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

FAU_STG.2	**Guarantees of audit data availability**
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.2.1:	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2:	The TSF shall be able to **[selection, choose one of: prevent]** unauthorised modifications to the stored audit records in the audit trail.
FAU_STG.2.3:	The TSF shall ensure that [assignment: metric for saving audit records] stored audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack]

PP Author Note: Preventing deletion and modification in software level can't always be guaranteed in software level. It sometimes requires cooperation of operating system and storage unit. But some types of the TOE work on a separate device, which is fully controllable by the TSF. This component shall be restricted to the capabilities of the TSF.

Rationale: *This component protects audit records against unauthorized deletion. This component makes contribution to O.AUDITsecurity objective.*

FAU_STG.3	**Action in case of possible audit data loss**
Hierarchical to:	No other components.
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1:	The TSF shall **[assignment: use a communication channel, SMS or equivalent, inform specifically granted users via system interfaces]** if the audit trail exceeds [assignment: a pre-defined limit].

Rationale: *This component defines the actions to be taken in case of an audit data loss. It also helps System_Administrator be informed about the situation. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

FAU_STG.4	**Prevention of audit data loss**
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1:	The TSF shall **[selection: send stored audit records to external archival unit, if the archival unit is also full, then provide specifically granted users with an option to move oldest audit records to an alternative storage unit,** and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

Application Note: Turkish Law requires that information systems belong to or regulated by the Turkish Government shall keep all audit records for a period of time. Since this is an obligation, there is no way of deletion of older audit records to keep newer ones. Alternative storage unit may be any internal or external unit capable of storing information (like external HDD, DVD, etc.)

Rationale: *This component aims to minimize the loss in case of the fact that audit trail is full. This component makes contribution to O.AUDIT and O.MANAGEMENT security objectives.*

6.1.5. CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_CKM.1	**Cyrptographic key generation**
Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 … or FCS_COP.1 Cyptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1:	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

FCS_CKM.4	**Cyrptographic key destruction**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 … or FDP_ITC.2 … or FCS_COP.1 Cyptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1:	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

What shall be international standards about cryptographic key destruction?

FCS_COP.1(1)	**Cyrptographic operation (Encryption)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(1):	The TSF shall perform **[assignment: audit data integrity verification]** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

PP Author Note: Methods for ensuring audit data integrity is left to ST Author. ST Author shall include additional components if they are needed for data integrity.

> ***Rationale:*** *This component introduces features for audit data integrity. This component makes contribution to O.DATA_INTEGRITY security objective.*

FCS_COP.1(2)	Cyrptographic operation (Generation of Hash Values)
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1(2):	The TSF shall perform **[assignment: hash data generation]** in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes **[assignment: none]** that meet the following: [assignment: list of standards].

Application Note: Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.1 and FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.

> ***Rationale:*** *This component introduces features for audit data integrity. This feature may also be used for securing authentication data. This component makes contribution to O.DATA_INTEGRITY, O.AUTH and O.AUDIT security objectives.*

6.1.6. CLASS FDP: USER DATA PROTECTION

FDP_ACC.2	Complete access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 …
FDP_ACC.2.1:	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2:	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1	Complete access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 …
FDP_ACC.2.1:	The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2:	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_IFC.1	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_ACC.1.1:	The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

PP Author Note: List of operations between subjects and objects should contain creation of a new object, removal of an object, all accesses including 38os ma methods, operations on TSF data binded to the object (for instance, 38os ma control list binded to the object). If a 38os mar all of these operations are defined in SRFs, then ST author should support the readers with sufficient explanation. If there is a need to define more than one 38os ma control policy, then ST author should FDP_ACC.1 should be repeated for every new 38os ma control policy.

> ***Rationale:*** *This component defines the information 38os ma control policy and specifies the methods of rights-based 38os ma control. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

FDP_IFF.1	
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset 38os ma control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1:	The TSF shall enforce the **[assignment: Access Control Policy]** to objects based on the following: **[assignment:** **a) User identity** **b) Roles and rights of the authenticated user,** **c) Cross-check mechanism ensuring that the user uses appropriate methods from appropriate sources when requesting a web page or a method,** **d) User session information and parameters sent with the request,** **e)** [Assignment: Other attributes of the subject] **].**
FDP_ACF.1.2:	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: Operation is only allowed if Access Control List has a record that gives right to the user with User ID or associated Group ID or user's role definition to 38os ma the object]**.
FDP_ACF.1.3:	The TSF shall explicitly authorise 38os ma of subjects to objects based on the following additional rules: **[assignment:** **a) Users having System_Administrator privileges have 38os ma to any records and methods provided by the TSF.** **b) Unauthorized users have 38os ma to any publicly available information without needing an authentication process.** **c)** [Assignment: other rules] **].**
FDP_ACF.1.4:	The TSF shall explicitly deny 38os ma of subjects to objects based on the following additional rules: **[assignment:** **a) Unexpectedly high number of requests from one or more specific Ips.** **b) Authentication attempts of a specific user exceeding pre-defined treshold**

	value. **c) Unexpectedly high number of requests coming from an authorized user** **d) Multiple sessions started by the same user that exceeds pre-defined treshold value.** **e)** [assignment: other rules] **].**

PP Author Note: Some systems may prefer to keep track of location of an authenticated user. If there is a significant change in the location of the user, then the system may require additional authentication information before authenticating the user. Since this method needs convertion of IP-ranges to location information, it is not included as an additional rule. But ST author may include this additional security feature.

Application Note: Precautions in software level are usually not enough to sufficiently prevent denial of service threats. Hence, a distinction made between DoS and DdoS threats. While some measures for DoS has been included in this protection profile, A.DIST_DENIAL_OF_SERVICE assumption is used for covering all types of denial of service attacks.

Rationale: *This component defines the details of the 39os ma control policy defined in FDP_ACC.1. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

FDP_RIP.2	**Full residual information protection**
Hierarchical to:	FDP_RIP.1 Subset residual information protection
Dependencies:	No dependencies.
FDP_RIP.2.1:	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects.

Rationale: *This component aims to protect residual information on the TOE. Protection of residual information is the core feature of a residual data management mechanism. This component makes contribution to O.RESIDUAL_DATA_MNG security objective.*

FDP_ITC.2	**Import of user data with security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset 39os ma control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1:	The TSF shall enforce the **[assignment: Access Control Policy]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2:	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3:	The TSF shall ensure that the protocol used provides 39os mar unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4:	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5:	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: When importing electronic records, TOE**

	shall verify integrity of the records by using e-signature verification].

Rationale: *This component aims to provide a functionality to verify imported data. This component makes contribution to O.DATA_FLOW_CONTROL and O.DATA_INTEGRITY security objectives.*

FDP_ETC.2	**Export of user data with security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset 40os ma control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1:	The TSF shall enforce the **[assignment: Access Control Policy]** when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2:	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3:	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4:	The TSF shall enforce the following rules when user data is exported from the TOE: **[assignment: System_Administrator shall restrict exporting of records, so that users of the TOE are not able to carry out an export operation without a reasonable aim]**.

Rationale: *This component aims to provide a functionality to apply some security measures for exported data. This component makes contribution to O.DATA_FLOW_CONTROL security objective.*

FDP_SDI.2	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1:	**Refinement:**The TSF shall 40os mar user data stored in containers controlled by the TSF for [assignment: integrity errors] ~~on all objects~~ **record data and audit data**, based on the following attributes: **[assignment: hash of stored user data]**.
FDP_SDI.2.2:	Upon detection of a data integrity error, the TSF shall [assignment: action to be taken].

Rationale: *This component aims to provide a functionality to verify the integrity of TSF data. This component makes contribution to O.DATA_INTEGRITY security objective.*

6.1.7. CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_AFL.1	**Authentication failure handling**

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1:	The TSF shall detect when [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] unsuccessful authentication attempts 41os related to **[assignment: user attempting to authenticate]**.
FIA_AFL.1.2:	When the defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: prevent 41os ma to TOE functions]**.

PP Author Note: When the defined number of unsuccessful authentication attempts has been met, it is secure to prevent the 41os ma to TOE functions. But it can easily be abused by users and may cause administrative overload. In addition to blocking 41os ma to TOE functions, the TOE may prefer to provide the user with an alternative authentication method like SMS verification, so that the user can continue to work without an interruption, without waiting 41os mar account to be unblocked.

Rationale: *This component protects the TOE against 41os m-force attacks by introducing a protection mechanism. This component makes contribution to O.AUTH security objective.*

FIA_ATD.1	**User attribute definition**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_ATD.1.1:	The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment:** **a) User identity code (user id) or PIN/password for Turkish Smart Identity Card** **b) Authentication method used** **c) Verification information for authentication method used** **d) Assigned roles of the user** **e) Status of the account of the user (active, passive, blocked, etc.)** **f)** [assignment: other security attributes] **]**.

Rationale: *This component defines the security attributes belonging to the users of the TOE. Security attributes are associated with the user during Authentication phase and kept in the TOE afterwards (until the session ends or longer, depending on the design of the TOE). This component makes contribution to O.AUTH security objective.*

FIA_SOS.1	**Verification of secrets**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1:	The TSF shall provide a mechanism to verify that secrets meet **[assignment:** **a) Should contain at least one uppercase letter,** **b) Should contain at least one lowercase letter,** **c) Should contain at least one number,** **d) Should contain at least one symbol,** **e) Should be at least 7 characters long,** **f) Should not contain repetitive or iterative character groups,**

	g) When changed, should not be the same as last 3 secrets. **h)** [assignment: other quality metrics] **]**.

PP Author Note: If the TOE prefers using stronger authentication mechanisms like Turkish Republic Smart Identity Card, e-Signature Token, Biometric Verification, etc., then this component may be fully ignored. In such situations, ST Author shall demonstrate that preferred verification mechanism provides a verification that is stronger than what is offered by this component.

Rationale: *This component defines the rules for secrets. These rules contributes to the measures taken against unauthorized 42os ma. This component makes contribution to O.AUTH security objective.*

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1:	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Rationale: *This component defines the rules 42os mar timing of authentication. This component makes contribution to O.AUTH security objective.*

FIA_UAU.7	**Protected authentication feedback**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1:	The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

Rationale: *This component requires that the TOE has multiple authentication mechanisms. Multiple authentication makes unauthorized 42 os ma harder. This component makes contribution to O.AUTH security objective.*

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1:	The TSF shall allow **[assignment:** **a) e-Signature verification page 42os mar records, which is offered to the receivers of the record (they don't need to be authorized to view the e-signature).** **b) Request for help on the login procedure** **]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2:	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Rationale: *This component defines which actions require authentication. This component makes contribution to O.AUTH security objective.*

FIA_USB.1	**User-subject binding**
Hierarchical to:	No other components.
Dependencies:	FIA_ATD.1 User attribute definition
FIA_USB.1.1:	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment:** **a) User identity code (user id)** **b) Roles assigned to the user** **c) Client interface details** **d) Authentication history (time of last successful and unsuccessful authentication attempts)** **e) Recent record/document 43os ma history** **f)** [assignment: list of other user security attributes] **]**.
FIA_USB.1.2:	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment:** **a) A clear session shall be established, information exists from the previous sessions shall be removed,** **b) Authentication history information shall be updated,** **c)** [assignment: other rules 43os mar initial association of attributes] **]**.
FIA_USB.1.3:	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: no change is allowed during an active session]**.

Rationale: *This component explains the details about user and subject binding. Since user attributes are also identified in this component, this component is complementary to auditing components. This component makes contribution to O.AUTH security objective.*

6.1.8. CLASS FMT: SECURITY MANAGEMENT

FMT_MOF.1	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MOF.1.1:	The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions **[assignment: all functions related with the management of the TOE]** to **[assignment: System_Administrator]**.

Rationale: *This component restricts the ability to manage security features to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MSA.1	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset 44os ma control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MSA.1.1:	The TSF shall enforce the **[assignment: Access Control Policy,** [assignment: other 44os ma control SFP(s)]**]** to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes **[assignment: list of security attributes defined in FIA_USB.1.1]** to **[assignment: System_Administrator]**.

Rationale: *This component restricts the ability to manage security attributes to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MSA.3	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1:	The TSF shall enforce the **[assignment: Access Control Policy]** to provide **[selection: restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2:	The TSF shall allow the **[assignment: System_Administrator]** to specify alternative initial values to override the default values when an object or information is created.

Rationale: *This component restricts the ability to manage security attributes to the authenticated System_Administrator. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MTD.1(1)	**Management of TSF data (System_Administrator)**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1(1):	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: **create,** other operations]] the [assignment: list of TSF data] to **[assignment: System_Administrator]**.

Rationale: *This component lets users authorized by the TOE to manage TSF data within the rules. This component makes contribution to O.MANAGEMENT security objective.*

FMT_MTD.1(2)	**Management of TSF data (Normal_User, Data_Entry_Operator)**
Hierarchical to:	No other components.

Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1(2):	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: **create,** other operations]] the **[assignment: TSF data that is under the ownership of a Normal_User or Data_Entry_Operator]** to **[assignment: Owning Normal_User or Data_Entry_Operator]**.

PP Author Note: If other users are also involved in the data, then there may be some restrictions on the allowed operations on the data.

Rationale: *This component lets users authorized by the TOE to manage TSF data within the rules. This component makes contribution to O.MANAGEMENT security objective.*

FMT_SMF.1	**Specification of management functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF, which are listed in Table 4]**.

Application Note: The list of management actions in Table 4 is a collection of management actions defined under component definitions in Common Criteria Standard – Part 2. Please refer to the Part 2 of the Standard for further information.

Rationale: *This component defines management actions on the TOE for chosen components. This component makes contribution to O.MANAGEMENT security objective.*

Table 4: List of Security Management Functions Provided by the TSF

Component*	**Management Action**
FAU_ARP.1	a) the management (addition, removal, or modification) of actions.
FAU_SAA.1	a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.
FAU_SAA.4	a) maintenance (deletion, modification, addition) of the subset of system events; b) maintenance (deletion, modification, addition) of the set of sequence of system events.
FAU_SAR.1	a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.
FAU_STG.2	a) maintenance of the parameters that control the audit storage capability.
FAU_STG.3	a) maintenance of the threshold; b) maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.

FAU_STG.4	a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
FDP_ACF.1	a) Managing the attributes used to make explicit access or denial based decisions.
FDP_DAU.1	a) The assignment or modification of the objects for which data authentication may apply could be configurable.
FDP_IFF.1	a) Managing the attributes used to make explicit access based decisions.
FDP_RIP.2	a) The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.
FIA_AFL.1	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure.
FIA_ATD.1	a) if so indicated in the assignment, the authorised administrator might be able to define additional security attributes for users.
FIA_SOS.1	a) the management of the metric used to verify the secrets.
FIA_UAU.2	a) management of the authentication data by an administrator; b) management of the authentication data by the user associated with this data.
FIA_UID.2	a) the management of the user identities.
FMT_MOF.1	a) managing the group of roles that can interact with the functions in the TSF.
FMT_MSA.1	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.
FMT_MSA.3	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given 46os ma control SFP; c) management of rules by which security attributes inherit specified values.
FMT_SMR.1	a) managing the group of users that are part of a role.
FPR_UNO.4	a) the list of authorised users that are capable of determining the occurrence of operations.
FPT_ITT.1	a) management of the types of modification against which the TSF should protect; b) management of the mechanism used to provide the protection of the data in transit between different parts of the TSF.
FPT_STM.1	a) management of the time.
FTA_MCS.2	a) management of the rules that govern the maximum allowed number of concurrent user sessions by an administrator.
FTA_SSL.1	a) specification of the time of user inactivity after which lock-out occurs for an individual user; b) specification of the default time of user inactivity after which lockout occurs; c) management of the events that should occur prior to unlocking the session.
FTP_ITC.1	a) Configuring the actions that require trusted channel, if supported.
FTP_TRP.1	a) Configuring the actions that require trusted path, if supported.

* No management actions has been foreseen for other components.

FMT_SMR.1	Security roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of authentication
FMT_SMR.1.1:	The TSF shall maintain the roles **[assignment:** **a) System_Administrator** **b) Normal_User** **c) Data_Entry_Operator** **d)** [assignment: other authorised identified roles] **]**.
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.

Rationale: *This component defines security roles 47os mar users. This component makes contribution to O.MANAGEMENT and O.AUTH security objectives.*

6.1.9. CLASS FPT: PROTECTION OF THE TSF

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1:	The TSF shall preserve a secure state when the following types of failures 47os : [assignment: application failures, user failures].

Rationale: *This component ensures that the TSF shall preserve a secure state in case of defined types of failures. This functionality is a core component of error management, besides it can help for a better TOE management as well. This component makes contribution to O.ERROR_MANAGEMENT security objective.*

FPT_TDC.1	Inter-TSF basic TSF data consistency
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TDC.1.1:	The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2:	The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.

ST Author Note: There are some circumstances that the TOE accepts data from external entities, like registered e-mail and database of government entities (DTVT Project of Turkey). For each of these entities, a new iteration has to be made to this component.

Rationale: *This component ensures a secure communication between the TOE and a trusted external IT entity. This component makes contribution to O.DATA_FLOW_CONTROL security objective.*

6.1.10. CLASS FRU: RESOURCE UTILISATION

FRU_FLT.1	**Degraded fault tolerance**
Hierarchical to:	No other components.
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1:	The TSF shall ensure the operation of **[assignment: all critical TOE capabilities]** when the following failures 48os : **[assignment: software failure,** [assignment: list of other type of failures]**].**

Application Note: "Critical" TOE capabilities mean any capability that is a part of the core functionality of the TOE. Software failures occuring because of hardware and/or operating system failures are out of scope.

Rationale: *This component ensures the operation of the TOE even some kind of failures 48os . Since audit records are important inputs for determining failures, this functionality is strongly related with O.AUDIT security objective. Besides, the functionality offered by this component is helpful for a better TOE management and error management. This component makes contribution to O.AUDIT and O.ERROR_MANAGEMENT security objectives.*

6.1.11. CLASS FTA: TOE ACCESS

FTA_MCS.1	**Basic limitation on multiple concurrent sessions**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of authentication
FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user.

PP Author Note: No determination has been made on the default number of sessions per user. However, if there is no need to provide a user with more than one session, it is recommended that only one active session is allowed for a user. If the TOE has a mobile interface as well, then maximum number of active sessions should be restricted to 2 or 3.

Rationale: *This component limits the number of multiple concurrent sessions for a user. This functionality helps for a better authentication. Besides, it prevents the Attacker to use residual data of an active session by initiating a parallel session. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

FTA_SSL.3	TSF-initiated termination
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1:	The TSF shall terminate an interactive session after a **[assignment: time interval of user inactivity that is defined by System_Administrator]**.

PP Author Note: ST author should be aware that background processing should also be taken into consideration when considering user inactivity time interval. After the determined time interval, user session should be terminated regardless of background processes binded to that specific user. Time interval should not be too long to allow the Attacker to give harm, but also should not be too short, as it may prevent rational use.

Rationale: *This component defines a time period for inactivity of the users. This functionality protects authenticated users and provides a mechanism against unwanted use of residual data. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

FTA_SSL.4	User-initiated termination
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4.1:	The TSF shall allow user-initiated termination of the user's own interactive session.

Rationale: *This component provides the user with a mechanism to protect his/her session data. Management of session data is a part of authentication and it is also a kind of residual data. This component makes contribution to O.AUTH and O.RESIDUAL_DATA_MNG security objectives.*

FTA_TAH.1	TOE 49os ma history
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TAH.1.1	**Refinement:** Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last **three** successful session establishment to the user.
FTA_TAH.1.2	Upon successful session establishment, the TSF shall display the [selection: date, time, method, location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.
FTA_TAH.1.3	The TSF shall not erase the 49os ma history information from the user interface without giving the user an opportunity to review the information.

Application Note: In FTA_TAH.1.1 and FTA_TAH1.2; "Method" means communication protocol/method used. It may have values like ftp, http, etc. Access from different mediums like desktop and mobile shall also be indicated in this column.

Rationale: *This component provides authorized users with previous successful authentication information, so that they may determine possible misuse of their user*

account. This functionality provides a method to prevent unauthorized 50os ma. This component makes contribution to O.AUTH security objective.

FTA_TSE.1	**TOE session establishment**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TSE.1.1:	The TSF shall be able to deny session establishment based on **[assignment:** **a) Location** **b) Port number** **c) Number of unsuccessful authentication attempts** **d) User ID, Role of the user or any other security attributes which define users** **e) Time range** **f) IP range** **g)** [assignment: any other attributes] **]**.

Application Note: Denial of session establishment based on time range means that some users may be given 50os ma to the TOE for a specific time period. This can be a definite time period, or any repeating time interval. This is especially useful for third party users of the TOE. This constraint provides protection against actions that 50os at a time where proper monitoring may not be in place.

Rationale: *This component defines restrictions on session establishment request of the users. This component makes contribution to O.AUTH and O.MANAGEMENT security objectives.*

6.2. SECURITY ASSURANCE REQUIREMENTS

This protection profile includes all Security Assurance Requirements defined in Common Criteria Part 3, EAL level 2. In addition to this, this protection profile also take into account following points:

ASE_CCL.1.10C section of ASE_CCL.1, which is defined in Common Criteria Part 3, has been rewriten to include "PP Author Note" subtitles of the included components. The new content is:

ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed. **When determining and verifying conformance claim rationale, subtitles named "PP Author Note" (if exist) should also be taken into account.**

Security Assurance Requirements of EAL 2 assurance level, extended with ALC_FLR.1 and ALC_LCD.1 has been shown in the table below (Table 5).

Table 5: List of Security Assurance Requirements

Assurance Class	**Component Definition**	**Component**
ADV: Development	Security architecture description	ADV_ARC.1
	Security-enforcing functional specification	ADV_FSP.2

	Basic design	ADV_TDS.1
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life-cycle support	Use of a CM system	ALC_CMC.2
	Parts of the TOE CM coverage	ALC_CMS.2
	Delivery procedures	ALC_DEL.1
	Basic flaw remediation	ALC_FLR.1
	Developer defined life-cycle model	ALC_LCD.1
ASE: Security Target evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST Introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	TOE summary specification	ASE_TSS.1
ATE: Tests	Evidence of coverage	ATE_COV.1
	Functional testing	ATE_FUN.1
	Independent testing – sample	ATE_IND.2
AVA: Vulnerability assessment	Vulnerability analysis	AVA_VAN.2

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. DEPENDENCIES OF SECURITY FUNCTIONAL REQUIREMENTS

Table 6 lists the dependencies of Security Functional Requirements and how they are included.

Table 6: List of the Dependencies of Security Functional Requirements

Component	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FAU_GEN.1 requires that FPT_STM.1 is included as a component. However, the TOE is not capable of providing this functionality. This functionality will be proovided by a trusted server. Hence, FPT_STM.1 is not included.
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1 FIA_UID.1

FAU_SAR.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1 Audit review	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1 Audit review	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data	FAU_GEN.1 FMT_MTD.1(1) FMT_MTD.1(2)
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FAU_STG.4	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FCS_COP.1(1)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Methods for ensuring audit data and record data integrity is left to ST Author. ST Author shall include additional components if they are needed for data integrity. FCS_CKM.4 component 52os ma may not be needed, according to data integrity method chosen by the ST Author.
FCS_COP.1(2)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.1 and FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys.
FDP_ACC.1	FDP_ACF.1 Security attribute based 52os ma control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset 52os ma control FMT_MSA.3 Static attribute	FDP_ACC.1 FMT_MSA.1
FDP_RIP.2	-	-
FDP_ITC.2	[FDP_ACC.1 Subset 52os ma control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1 FPT_TDC.1 FPT_ITC.1 or FTP_TRP.1 is not included, since this P.SSL_COMMUNICATION already provides a secure channel between TOE and external entities.
FDP_ETC.2	[FDP_ACC.1 Subset 52os ma control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1
FDP_SDI.2	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	-	-
FIA_SOS.1	-	-

FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.5	-	-
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 Subset 53os ma control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.1
FPT_FLS.1	-	-
FPT_TDC.1	-	-
FRU_FLT.1	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1
FTA_MCS.1	FIA_UID.1 Timing of identification	FIA_UID.1
FTA_SSL.3	-	-
FTA_SSL.4	-	-
FTA_TAH.1	-	-
FTA_TSE.1	-	-

6.3.2. DEPENDENCIES OF SECURITY ASSURANCE REQUIREMENTS

Table 7 lists the dependencies of Security Assurance Requirements and how they are included.

Table 7: List of the Dependencies of Security Assurance Requirements

Component	Dependency	Inclusion
ADV_ARC.1	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design	ADV_FSP.1 ADV_TDS.1

ADV_FSP.2	ADV_TDS.1 Basic design	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2 Security enforcing functional specification	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1
AGD_PRE.1	-	
ALC_CMC.2	ALC_CMS.1 TOE CM coverage	ALC_CMS.1
ALC_CMS.2	-	
ALC_DEL.1	-	
ALC_FLR.1	-	
ALC_LCD.1	-	
ASE_CCL.1	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements	ASE_INT.1 ASE_ECD.1 ASE_REQ.1
ASE_ECD.1	-	
ASE_INT.1	-	
ASE_OBJ.2	ASE_SPD.1 Security problem definition	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition	ASE_OBJ.2 ASE_ECD.1
ASE_TSS.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ASE_REQ.1 ADV_FSP.1
ATE_COV.1	ADV_FSP.2 Security enforcing functional specification ATE_FUN.1 Functional testing	ADV_FSP.2 ATE_FUN.1
ATE_FUN.1	ATE_COV.1 Evidence of coverage	ATE_COV.1
ATE_IND.2	ADV_FSP.2 Security enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 Security architecture description ADV_FSP.2 Security enforcing functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1

6.3.3. SCOPE OF SECURITY FUNCTIONAL REQUIREMENTS

Table 8 presents a mapping of SFRs and security objectives. Every SFR corresponds to at least one security objective. Similarly, every security objective corresponds to at least one SFR. The table also verifies that chosen SFRs are required and they are sufficiently addressing all security objectives.

6.3.4. RATIONALE OF EAL PACKAGE

When choosing EAL level, security requirements of the document and record management system applications has been considered. These applications require a moderate level of security. Attack potential is relatively low, when compared 55os mart cards and/or banking applications.

Another consideration made during EAL decision is relatively more frequent update needs of web-based applications. Since web-based applications can be reached from the internet and internet threats change quickly, they should be reflected to the products as fast as possible. A higher assurance level would need longer certification periods, which may result in a shrinking demand.

Table 8: Coverage of Security Functional Requirements

RESOURCES

Nist special publication 800-53

Ids analyzer pp

Network devices pp

Kore ips pp

gartner raporu