RSA, The Security Division of EMC

RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.5

Prepared for:

RSA, The Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730
United States of America

Phone: +1 (877) RSA-4900

http://www.rsa.com

Prepared by:

Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267-6050

http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3, and will hereafter be referred to as the TOE throughout this document. The TOE is a risk-based authentication system that provides additional layers of security to organizations with a web presence. The TOE provides additional authentication measures using user credentials, positive device identification, and risk analysis during login and continuously during transaction processing.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	RSA, The Security Division of EMC RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Security Target
ST Version	Version 0.5
ST Author	Corsec Security, Inc.
ST Publication Date	3/31/2011
TOE Reference	RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Patch 0 Hot Fix 0
FIPS[1] 140-2 Status	Level 1, Validated crypto module, Certificate No. 1048

[1] FIPS – Federal Information Processing Standard

ST Title	RSA, The Security Division of EMC RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Security Target
Keywords	RSA, EMC, Adaptive Authentication

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The RSA Adaptive Authentication (AA) System is a risk-based authentication platform that provides additional layers of security to companies with an online presence. The RSA AA System uses positive device identification and risk analysis to ensure that only genuine online customers can access their accounts. The RSA AA System provides additional authentication measures during login and continuous monitoring of each transaction. If a single transaction (or series of transactions) increases the perceived risk level, the online customer may be challenged to provide additional authentication, or the transaction can be flagged for later review.

Figure 1 shows one possible deployment configuration of the RSA AA System:

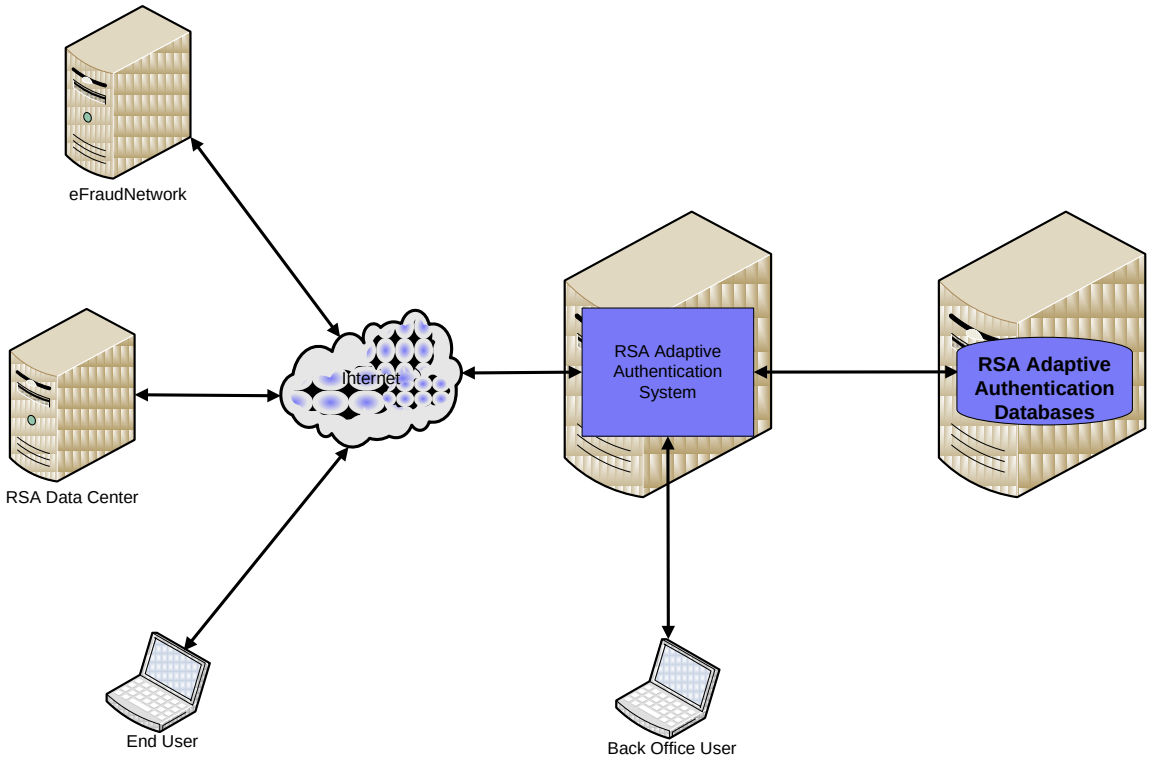

Figure 1 - Deployment Configuration of the RSA AA System

1.3.1 Brief Description of the Components of the RSA AA System

The RSA AA System is composed of several parts that are primarily written in Java. The product can be distributed across several servers or deployed with all the product components installed on a single server. The product can be divided into the following major components, as shown in Figure 2 below:

- Core Components
- Back Office Applications
- Adaptive Authentication Utilities
- Data and Configuration Databases
- External Network Interfaces

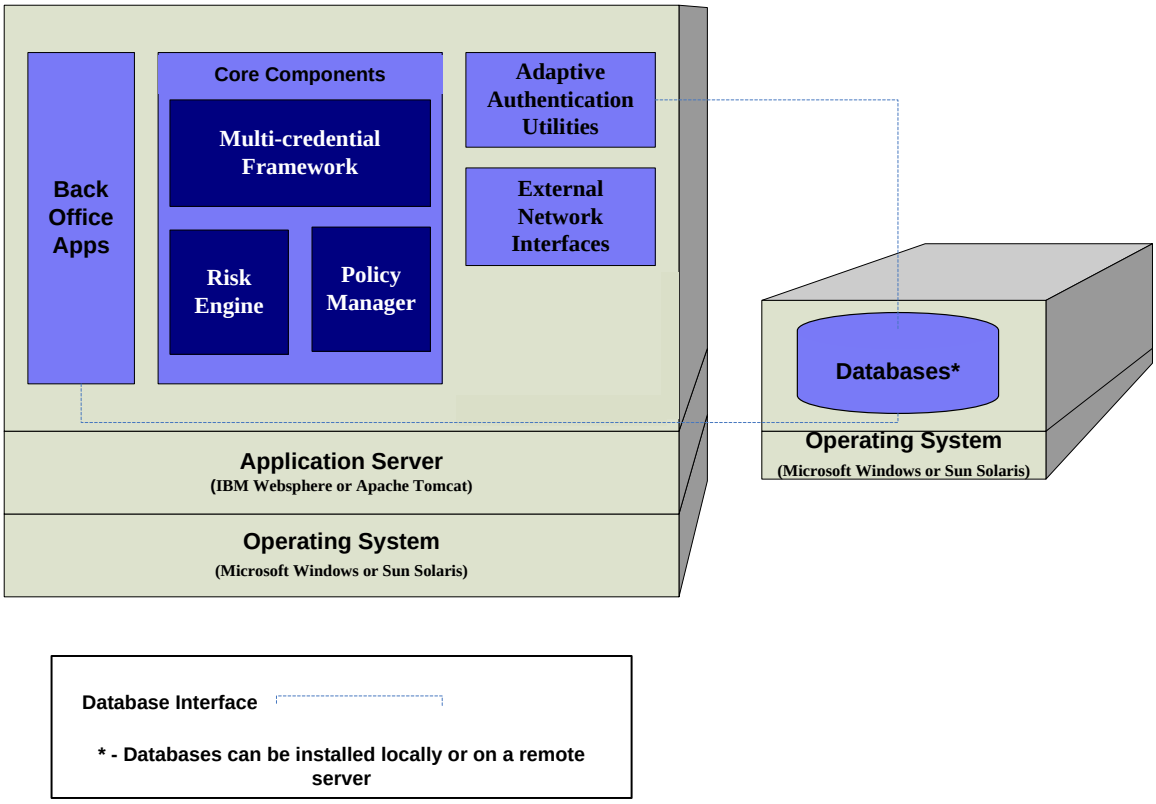

Figure 2 – RSA AA System Components

The Core Components provide the fundamental functionality of transaction risk assessment, authentication processing based on risk, and transaction policies enforcement. The Risk Engine, Policy Manager, and Multi-credential Framework make up the Core Components. An online website that relies on the RSA AA System will send individual transactions to the product via SOAP messages conveyed using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). Transactions can be initial authentication requests or other specific transaction events from the online application. All transactions enter the product over the Adaptive Authentication Web Services Interface, a well-defined application programming interface (API) for Web Services using Web Services Description Language (WSDL). The Risk Engine takes information from a variety of sources, including the online application, and performs a risk analysis to determine how much risk a transaction presents. The risk score from the Risk Engine is used as an input to the Policy Manager. The Policy Manager enforces the transaction handling policies that are defined by the system administrators. The policy decision trees will result in a decision of Allow, Deny, Challenge, or Review for each transaction the RSA AA System processes. If a policy decision of Challenge is reached, the RSA AA System can provide several additional authentication mechanisms to authenticate the online customer. The product can provide challenge questions or require an out-of-band action such as a response to an e-mail or phone call to authenticate the customer.

This product supports two types of users. There are Back Office Users who are the administrators of the product. Back Office Users will configure and maintain the system and enter the policies that the product

will enforce. There are also End Users who are the online customers that will be subjected to the authentication policies.

Administrators of the RSA AA System administer the device using a set of Back Office Applications. The Access Management Tool, Report Viewer, Customer Service Representative (CSR) Tool, Policy Editor, Administration Console, and Case Management Tool applications make up the Back Office Applications. The Access Management Tool provides a single interface for access to the other Back Office applications. It allows administrators to create Back Office Users and manage roles and permissions for the different Back Office applications, and provides a method for configuring organizations and groups. The Report Viewer allows administrators to view daily, weekly, or monthly reports created by the RSA Data Center; the Report Viewer does not generate reports. The CSR Tool is designed to help CSRs look up and modify user account information as the user interacts with the RSA AA System. The Policy Editor allows Back Office Users to configure and customize the necessary policies by which the RSA AA System detects and challenges potentially risky End Users, marks transactions for review by Fraud Analysts, allows valid End Users, or denies fraudulent End Users. The Admin Tool, which is part of the Policy Editor, can be used to add, remove, and save elements from security risk lists such as country or Internet Protocol (IP) blacklists, watch lists, and white lists. The Administration Console is used to control the system configurations and provides a set of system health checks. The Case Management Tool is used to review any events that have been flagged as risky by the RSA AA System, and requires review by a Fraud Analyst.

There are a number Adaptive Authentication Utilities that run in the background or provide specific configuration tools for the RSA AA System. These utilities can be used by administrators to help manage the RSA AA System and troubleshoot any problems. The following utilities are included in the Adaptive Authentication Utilities:

- Health Check Servlet
- Simple Mail Transfer Protocol (SMTP) and HTTP[2] to Voice Extensible Markup Language (VXML) or Telephony
- Aggregator Token Generator
- Log Manager
- Policy Simulator
- Billing Utility
- GeoIP Admin Tool
- GeoIP Inspector Utility
- Risk Engine Offline Task Utility
- Scheduler

The RSA AA System utilities utilize three primary data stores: Tools Database, Case Management Database, and the AA Database. The Tools Database stores the authentication credentials and privileges for the administrators that authenticate and use the Back Office Applications. The Case Management Database contains events that have been flagged as risky by the RSA AA System, and requires review by a Fraud Analyst. The AA Database is the primary data store for the Core Components. It contains the policy table information for the Policy Manager and the End User credentials other than user name and password, including secret questions and responses and site-to-user authentication data. Site-to-user authentication uses a personal security image and caption that is pre-selected by the customer during registration to provide assurance that a website is genuine before the customer proceeds to enter confidential or sensitive personal information to the site. The RSA AA System provides encryption of End User credentials, including answers to secret challenge questions and site-to-user phrases encrypted in the databases.

[2] HTTP – Hypertext Transfer Protocol

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The software-only TOE comprises all features and functionality contained within the Core Components, Back Office Applications, Adaptive Authentication Utilities, and External Network Interfaces components of the RSA AA System as describe above in Section 1.3. Only the Data and Configuration Databases are excluded from the TOE.

RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Patch 0 Hot Fix 0 (a unique build) is the evaluated version of the product.

1.4.1 TOE Environment

The TOE is intended to be deployed on a general purpose computer (GPC) in a physically secured room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.). The TOE is intended to be managed by administrators operating under a consistent security policy.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The RSA AA System is a risk-based authentication application that executes on a GPC. The essential physical components for the proper operation of the TOE in the evaluated configuration consist of the GPC software and hardware, and the RSA AA System Databases. The GPC (in particular, the resident operating system and networking components) provides the basic operating system functions, such as system resource management and communications between the hardware and software, plus other core functionality, such as object store, network stack, etc.

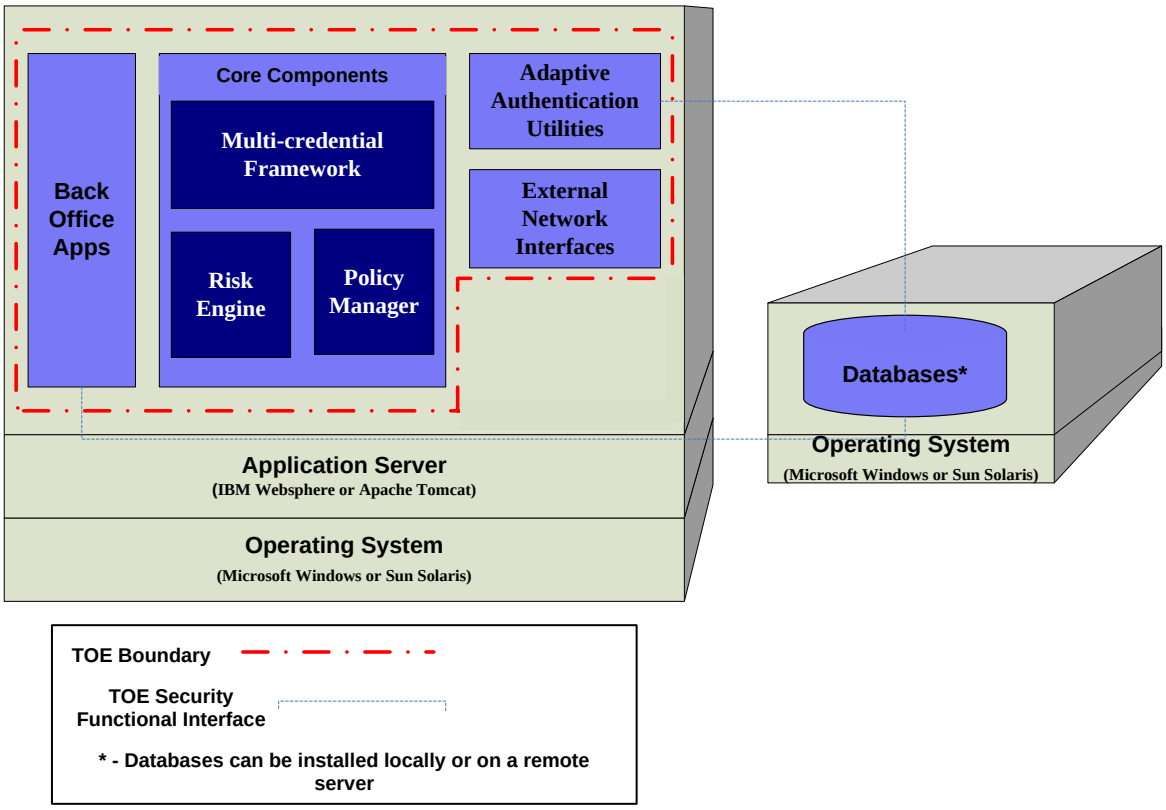

Figure 3 - Physical TOE Boundary

1.5.1.1 TOE Software

The RSA AA System is a software TOE that requires an application server to run. The product will run with IBM Websphere, Apache Tomcat, JBoss, or BEA Weblogic application servers. With an application server providing a Java runtime environment, the product can be installed on numerous versions of IBM AIX, Microsoft Windows, Linux, and Sun Solaris operating systems. The product can be distributed across several servers or deployed with all the product components installed on a single server. The RSA AA System relies on the presence of a database application to store data and configurations. The RSA AA System supports the use of Microsoft SQL[3] Server, Oracle (Windows or Linux versions), and IBM DB2 (Windows, Linux, or AIX versions).

For this evaluation, the TOE will be installed on a single server, with databases resident on a separate machine. The following external environmental components comprise the evaluated configurations of the TOE:

- Operating systems: Microsoft Windows Server 2003; Microsoft Windows Server 2003 R2; Microsoft Windows Server 2008; Microsoft Windows Server 2008 R2; Oracle Solaris 10
- Application servers: IBM Websphere 7.0; Apache Tomcat 6.0; Red Hat JBoss 5.1
- Database applications: Oracle 11g; Microsoft SQL Server 2005; Microsoft SQL Server 2008; IBM DB2 9.7

[3] SQL – Structured Query Language

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Access Management User's Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Authentication Plug-In Developer's Guide
- Architectural Overview RSA Adaptive Authentication for the Web v6.0.2.1. rev 1.5
- Best Practices for Challenge Questions
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Case Management User's Guide
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Configuration Framework Guide
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Customer Services Representative (CSR) Administration Guide
- RSA Diagnostics Manager 3.2 User Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Operations Guide
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Policy Editor User's Guide
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3 Policy Simulator User's Guide
- Release Notes RSA Adaptive Authentication (On-Premise) v6.0.2.1 SP3
- RSA Adaptive Authentication (On-Premise) v6.0.2.1 Reporting Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Web Services API Reference Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Workflow & Processes Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Integration Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 and RSA FraudAction Bait Credentials Setup and Implementation Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP2 Installation Guide
- RSA Adaptive Authentication (On-Premise) 6.0.2.1 SP3 Upgrade Guide
- RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 Guidance Supplement

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Case Recording and Review

1.5.2.1 Cryptographic Support

The TOE provides encryption of End User credentials, including answers to secret challenge questions and site-to-user phrases encrypted in the databases. The TOE also encrypts cookies used to bind a user to a device, as well as Authentication Credential Service Provider (ACSP) session data for Out-Of-Band (OOB) authentication. The Back Office applications use hashing functionality for password management and not encryption. The cryptographic functionality is provided by a FIPS 140-2-validated cryptographic module: RSA BSAFE Crypto-J JCE Provider Module v4.0, certificate #1048.

1.5.2.2 User Data Protection

The TOE provides authorized administrators with the ability to set up security policies using the Policy Manager. The Policy Manager provides for the creation of rules that define certain actions the TOE should take based on a set of conditions. These policies define the conditions under which End Users are required to provide additional authentication credentials.

1.5.2.3 Identification and Authentication

The TOE provides the ability for administrators to manage the security functions of the TOE and user access to TOE functionality. The identification and authentication security function ensures that access to configuration and management functionality available via the Back Office Tools component of the TOE is restricted to authorized TOE users and access is protected by the entry of credentials. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage.

End User authentication is supported by the RSA AA System's layered security approach. While initial logins are validated by the front-end application, the RSA AA System provides additional validation using information collected from each enrolled End User. Risk analysis is performed on logins (and other requested transactions) and recommendations are made regarding how to proceed. End Users who have not previously used the RSA AA System's services can be required by the front-end application to enroll in the RSA AA System, providing challenge questions to be used by the system to verify their identity later, and choosing a personal image and text phrase by which the End User can authenticate that they are connected to the correct front-end application.

1.5.2.4 Security Management

Upon installation, the TOE includes a default set of roles that have associated permissions. The roles and permissions define which administrators have access to which information. Authorized administrators can also create new roles and permission sets as required.

The Security Management function also provides administrators with the ability to properly manage and configure the TOE. TOE administrators can use the Policy Editor tool to create rules that control the flow of end user information.

1.5.2.5 Case Recording and Review

The TOE provides the means to monitor End User transactions for potentially fraudulent activities. Information from logins and transactions that are deemed potentially fraudulent can be generated and saved to a case log for later review by a Fraud Analyst.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

This evaluation includes all the physical/logical features and functionality available in the listed configuration(s) of the TOE, except for the eFraudNetwork Agent, which is disabled in the CC-evaluated configuration.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2010/07/30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ (Augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[4] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[5] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 3 - Threats

Name	Description
T.DOS	An attacker may attempt to flood the TOE with network traffic, rendering the TOE's services inaccessible to authorized users.
T.FRAUD	An attacker may take advantage of weak authentication mechanisms to commit fraudulent activities against the host application employing the TOE.
T.MASQUERADE	An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	An attacker may be able to bypass the TOE's security mechanisms by tampering with the TOE or the TOE environment.
T.UNAUTH	An attacker may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.

[4] IT – Information Technology
[5] TSF – TOE Security Functionality

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 4 - Organizational Security Policies

Name	Description
P.ADMIN	The TOE shall provide a set of tools for the secure management of TOE data and functions.
P.CASELOG	The TOE shall have the capability to record "high-risk" events and activities in a case log for later review.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from unauthorized deletion or modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.RECOMMEND	The TOE shall make recommendations regarding the submission of authentication credentials based on a calculated risk associated with the login attempt or transaction.
P.RISK	The TOE shall have the capability to compute a "risk factor" for a given end user login attempt or transaction.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 - Assumptions

Name	Description
A.AUDIT	The operating system that the TOE is installed on is correctly configured by the administrator to audit all administrative actions that the administrator deems necessary.
A.INSTALL	The TOE is properly installed on a hardware and operating system capable of supporting all of its required functionality.
A.LOCATE	The TOE is located within a controlled access facility
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides a private network that allows the TOE to provide its security functions to TOE components, the database server, front-end applications, and the RSA Data Center.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

Name	Description
A.PROTECT	The TOE software will be protected from unauthorized modification.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.
O.ADMIN_AUTH	The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.
O.ENDUSER_AUTH	The TOE must be able to identify and authenticate end users prior to allowing access to end user functions and data and high-risk transactions.
O.MONITOR	The TOE must provide a mechanism to continuously monitor end user transactions, and to record potentially risky transactions for later review.
O.RECOMMEND	The TOE must be able to make recommendations regarding the submission of authentication credentials based on a calculated risk associated with the login attempt or transaction.
O.RISK_FACTOR	The TOE must provide a mechanism for determining a "risk factor" of allowing a given login or transaction to be performed.
O.VALIDATED_CRYPTO	The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 cryptographic module.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 - IT Security Objectives

Name	Description
OE.AUDIT	The TOE environment will be configured to audit all administrative actions.
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.PLATFORM	The TOE hardware and Operating System must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.SECURE_COMMS	The TOE environment must ensure that communications between the TOE components, the database server, front-end applications, and the RSA Data Center are protected via a secure channel.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 - Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE

Table 9 - Extended TOE Security Functional Requirements

Name	Description
EXT_FCR_ARP.1	Security alarms
EXT_FCR_GEN.1	Case data generation
EXT_FCR_CDA.1	Potential violation analysis
EXT_FCR_CDA.2	Simple attack heuristics

5.1.1 Class EXT_FCR: Case Recording and Review

Case Recording and Review involves recognizing, recording, storing, and analyzing records of users committing potentially fraudulent activities against a TOE-protected system. The EXT_FCR: Case Recording and Review function class was modeled after the CC FAU: Security audit class. Table 10 lists the CC families after which the extended families within this class are modeled:

Table 10 – Class EXT_FCR Families

Extended Family	Modeled CC Family
EXT_FCR_ARP: Transaction automatic response	FAU_ARP: Security audit automatic response
EXT_FCR_GEN: Case data generation	FAU_GEN: Security audit data generation
EXT_FCR_CDA: Case data analysis	FAU_SAA: Security audit analysis

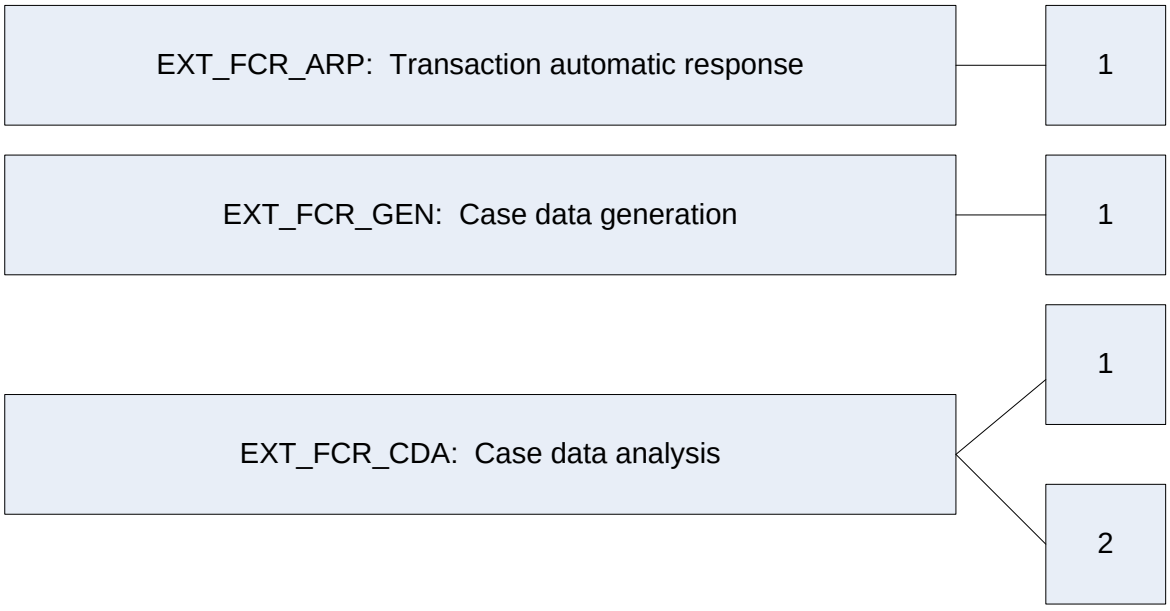

Figure 4 - EXT_FCR: Case Recording and Review Class Decomposition

5.1.1.1 Family EXT_FCR_ARP

Within the EXT_FCR_ARP family, there is one extended SFR, EXT_FCR_ARP.1, which was modeled after the CC SFR FAU_ARP.1.

5.1.1.1.1 Case automatic response (EXT_FCR_ARP)

Family Behaviour

This family defines the response to be taken in case of detected transactions indicative of potentially fraudulent activity.

Component Leveling

Figure 5 - EXT_FCR_ARP Transaction Automatic Response family decomposition

EXT_FCR_ARP.1 Security alarms shall take actions in case a potentially fraudulent activity is detected.

Management: EXT_FCR_ARP.1

The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions.

Audit: EXT_FCR_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Actions taken due to potential fraudulent activity.

EXT_FCR_ARP.1 Security alarms
Hierarchical to: No other components
EXT_FCR_ARP.1.1

The TSF shall make the recommendation [assignment: *list of recommendations that can be made*] upon determination of a heightened potential of risk for a given transaction.

Dependencies: EXT_FCR_CDA.1 Potential violation analysis

5.1.1.2 Family EXT_FCR_GEN

Within the EXT_FCR_GEN family, there is one extended SFR: EXT_FCR_GEN.1, which was modeled after the CC SFR FAU_GEN.1.

5.1.1.2.1 Case data generation (EXT_FCR_GEN)

Family Behaviour

This family defines the requirements for recording the occurrence of potentially fraudulent activities that take place against a TOE-protected system. This family enumerates the types of activities that shall be recorded by the TSF, and identifies the minimum set of transaction-related information that should be provided within various case record types.

Component Leveling

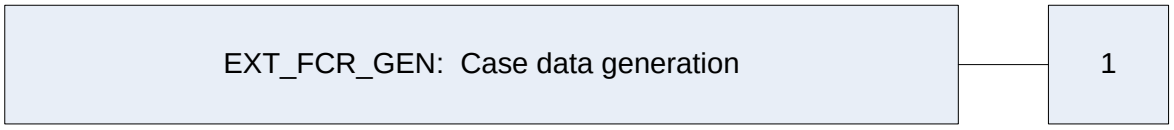

Figure 6 - EXT_FCR_GEN Case Data Generation family decomposition

EXT_FCR_GEN.1 Case data generation specifies the list of data that shall be monitored during transactions and recorded in the generation of a case.

Management: EXT_FCR_GEN.1

There are no management activities foreseen.

Audit: EXT_FCR_GEN.1

There are no auditable events foreseen.

EXT_FCR_GEN.1 Case data generation
Hierarchical to: No other components
EXT_FCR_GEN.1.1

The TSF shall be able to generate case data of the following monitored activities: [assignment: *list of activities that can be monitored*].

EXT_FCR_GEN.1.2

The TSF shall record within each record at least the following information: [assignment: *list of information stored in every generated case data record*].

Dependencies: No dependencies

5.1.1.3 Family EXT_FCR_CDA

Within the EXT_FCR_CDA family, there are two extended SFRs: EXT_FCR_CDA.1, which was modeled after the CC SFR FAU_SAA.1, and EXT_FCR_CDA.2, which was modeled after the CC SFR FAU_SAA.3.

5.1.1.3.1 Case data analysis (EXT_FCR_CDA)

Family Behaviour

This family defines requirements for automated means that analyze system activity and case data, looking for possible or real fraudulent activities. This analysis may work in support of intrusion detection or automatic response to a potentially fraudulent activity.

Component Leveling

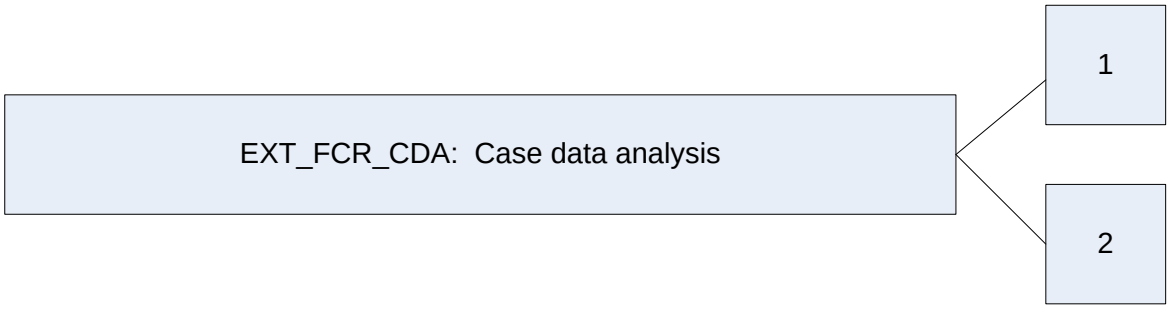

Figure 7 - EXT_FCR_CDA Case Data Analysis family decomposition

EXT_FCR_CDA.1 Potential violation analysis defines the basic threshold detection on the basis of a fixed rule set.

EXT_FCR_CDA.2 Simple attack heuristics shall be able to detect the occurrence of signature events that represent a potential threat against the TOE-protected system.

Management: EXT_FCR_CDA.1

The following actions could be considered for the management functions in FMT:

- The maintenance of the rules by (adding, modifying, or deletion) of rules from the set of rules.

Management: EXT_FCR_CDA.2

The following actions could be considered for the management functions in FMT:

- Maintenance (deletion, modification, or addition) of the subset of system events.

Audit: EXT_FCR_CDA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: enabling and disabling of any of the analysis mechanisms;
- Minimal: automated responses performed by the tool.

Audit: EXT_FCR_CDA.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: enabling and disabling of any of the analysis mechanisms;
- Minimal: automated responses performed by the tool.

EXT_FCR_CDA.1 Potential violation analysis
Hierarchical to: No other components
EXT_FCR_CDA.1.1

The TSF shall be able to apply a set of rules in monitoring on-going transactions and, based upon these rules, indicate a potentially fraudulent activity against the TOE-protected system.

EXT_FCR_CDA.1.2

The TSF shall enforce the following rules for monitoring on-going transactions:
a) Risk factor calculation based on user, device, and transaction data;
b) No other rules.

Dependencies: EXT_FCR_GEN.1 Case data generation

EXT_FCR_CDA.2 Simple attack heuristics
Hierarchical to: EXT_FCR_CDA.1 Potential violation analysis
EXT_FCR_CDA.2.1

The TSF shall be able to maintain an internal representation of the following risk information [assignment: *list of risk information used in determining risk level for a transaction*] that help in determining a level of risk for a given transaction.

EXT_FCR_CDA.2.2

The TSF shall be able to compare the stored risk information against information about the current transaction discernible from an examination of [assignment: *list of data gathered from the current transaction*].

EXT_FCR_CDA.2.3

The TSF shall be able to indicate an appropriate course of action for a given transaction when the level of risk for a transaction indicates a potentially fraudulent use of a TOE-protected system.

Dependencies: EXT_FCR_GEN.1 Case data generation

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance components associated with this evaluation.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1(a)	Subset access control		✓		✓
FDP_ACC.1(b)	Subset access control		✓		✓
FDP_ACF.1(a)	Security attribute based access control		✓		✓
FDP_ACF.1(b)	Security attribute based access control		✓		✓
FDP_ETC.1	Export of user data without security attributes		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_ITC.1	Import of user data without security attributes		✓		
FIA_ATD.1(a)	User attribute definition		✓	✓	✓
FIA_ATD.1(b)	User attribute definition		✓	✓	✓

Name	Description	S	A	R	I
FIA_SOS.1	Verification of secrets		✓	✓	
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action			✓	
FIA_UAU.5	Multiple authentication mechanisms		✓	✓	
FIA_UAU.6	Re-authenticating		✓	✓	
FIA_UAU.7	Protected authentication feedback		✓	✓	
FIA_UID.1	Timing of identification		✓	✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1(a)	Management of security functions behaviour	✓	✓		✓
FMT_MOF.1(b)	Management of security functions behaviour	✓	✓		✓
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.1(c)	Management of security attributes	✓	✓		✓
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1(a)	Management of TSF data	✓	✓		✓
FMT_MTD.1(b)	Management of TSF data	✓	✓		✓
FMT_MTD.1(c)	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
EXT_FCR_ARP.1	Security alarms		✓		
EXT_FCR_GEN.1	Case data generation		✓		
EXT_FCR_CDA.1	Potential violation analysis				
EXT_FCR_CDA.2	Simple attack heuristics		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*the cryptographic key generation algorithms as listed in the 'Key Generation Algorithm' column of Table 12*] and specified cryptographic key sizes [*listed in the 'Cryptographic Key Size' column of Table 12*] that meet the following: [*standards listed in the 'Standards' column of Table 12*].

Table 12- Cryptographic Key Generation Standards

Key Generation Algorithm	Cryptographic Key Size	Standards
PRNG[6]	All key sizes specified in the Key Sizes (bits) column of Table 13 below.	FIPS 186-2 with Change Notice 1 (Cert #389)
DSA [7]	All key sizes specified in the Key Sizes (bits) column of Table 13 below.	FIPS 186-2 (Cert #251)
ECDSA[8]	All key sizes specified in the Key Sizes (bits) column of Table 13 below.	X9.62/FIPS 186-2 with Change Notice 1 (Cert #72)
RSA[9]	All key sizes specified in the Key Sizes (bits) column of Table 13 below.	ANSI[10] X9.31 (Cert #311)

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or

[6] PRNG – Pseudo-Random Number Generator

[7] DSA – Digital Signature Algorithm

[8] ECDSA – Elliptic Curve Digital Signature Algorithm

[9] RSA – Rivest, Shamir, and Adleman

[10] ANSI – American National Standards Institute

FCS_CKM.1 Cryptographic key generation]

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 13*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 13*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 13*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 13*].

Table 13 - Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Cert #)
Symmetric encryption and decryption	AES[11] (ECB[12], CBC[13], CFB[14], OFB[15], CTR[16], CCM[17])	128, 192, 256	FIPS-197 (Cert #669)
	Triple-DES[18] (ECB, CBC, CFB, OFB)	Two-key, Three-key	FIPS 46-3 (Cert #614)
Message Digest/Hashing	SHA[19]	160, 224, 256, 384, 512	FIPS 180-3 (Cert #702)
Message Authentication	HMAC[20] SHA	160, 224, 256, 384, 512	FIPS 198 (Cert #353)
Pseudo-Random Number Generation	PRNG	n/a	FIPS 186-2 with Change Notice 1 (Cert #389)
Digital Signature Generation	DSA	1024	FIPS 186-2 (Cert #251)
	ECDSA	Curves: All-P, All-K, All-B	FIPS 186-2 with Change Notice 1 (Cert #72)
	RSA, PKCS[21]#1	1024, 1536, 2048, 3072, 4096	ANSI X9.31 (Cert #311)
Digital Signature Verification	DSA	1024	FIPS 186-2 (Cert #251)
	ECDSA	Curves: All-P, All-K, All-B	FIPS 186-2 with Change Notice 1 (Cert #72)
	RSA, PKCS#1	1024, 1536, 2048, 3072, 4096	ANSI X9.31 (Cert #311)

[11] AES – Advanced Encryption Standard

[12] ECB – Electronic Code Book

[13] CBC – Cipher-Block Chaining

[14] CFB – Cipher Feedback

[15] OFB – Output Feedback

[16] CTR – Counter

[17] CCM – Counter with CBC-MAC (Message Authentication Code)

[18] Triple-DES – Triple Data Encryption Standard

[19] SHA – Secure Hash Algorithm

[20] HMAC – Hashed-based Message Authentication Code

[21] PKCS – Public Key Cryptography Standards

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

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1(a)
The TSF shall enforce the [*Back Office User Access Control SFP*[22]] on [*TOE users accessing the Back Office Tools component of the TOE*].
Dependencies: FDP_ACF.1(a) Security attribute based access control

FDP_ACC.1(b) Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1(b)
The TSF shall enforce the [*End User Access Control SFP*] on [*users authenticating to a front-end application employing the TOE*].
Dependencies: FDP_ACF.1(b) Security attribute based access control

FDP_ACF.1(a) Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1(a)
The TSF shall enforce the [*Back Office User Access Control SFP*] to objects based on the following:
[
Back Office User (subject) attributes:
a. User name
b. Password
c. Assigned Back Office Tool(s)
d. Assigned role
e. Assigned operation(s) (create, read, update, delete)
Back Office Tool (object) attributes:
a. none].
FDP_ACF.1.2(a)
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
a. The user must have a valid user name and password.
b. The user must have permissions assigned by an administrator allowing access to the desired Back Office Tool (the "controlled objects").
c. The user's assigned role must support the operation they wish to perform.
].
FDP_ACF.1.3(a)
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].
FDP_ACF.1.4(a)
The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].
Dependencies: FDP_ACC.1(a) Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1(b) Security attribute based access control
Hierarchical to: No other components.

[22] SFP – Security Functional Policy

FDP_ACF.1.1(b)

The TSF shall enforce the [*End User Access Control SFP*] to objects based on the following:

[

a. *User name*
b. *Password*
c. *Challenge questions and answers*
d. *Out-of-Band authentication information*
e. *Network information*
f. *Device information*

Transaction (object and operation) attributes:

a. *Level of risk, as determined by the TOE Risk and Policy Engine*

].

FDP_ACF.1.2(b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

a. *(In "Sign-in with Risk-Based Authentication" deployment) The End User is allowed to perform an operation if:*
    1. *The TOE Risk and Policy Engine determines that the End User's characteristics (user name, password, challenge response, out-of-band response, network information, and device information) and the level of risk posed by the operation (i.e., transaction) are deemed acceptable (according to the current policy); or*
    2. *The End User's characteristics are deemed acceptable (according to the current policy) and an authentication challenge (due to a high level of risk) is successfully passed.*
b. *(In "Sign-in with Positive Device Identification Only" deployment) The End User is allowed to perform an operation if:*
    1. *The End User is authenticating from a device that is deemed acceptable (according to the current policy) through positive identification; or*
    2. *The End User is authenticating from an unknown device, but successfully passes an authentication challenge.*
c. *(In "Sign-in Monitoring" deployment) No rules.*

].[23]

Application Note: The term "acceptable" in this SFR means that the End User's characteristics and/or the operation's level of risk meet the requirements of the current policy set by the TOE Administrator.

FDP_ACF.1.3(b)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b)

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: FDP_ACC.1(b) Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

FDP_ETC.1.1

The TSF shall enforce the [*Back Office User Access Control SFP, and End User Access Control SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

[23] These deployments are defined in Section 7.1.2.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Transactional Information Flow Control SFP*] on

[

a. (subjects) End Users attempting to perform policy-controlled transactions
b. (information) End User authentication status
c. (operations) policy-controlled transactions

].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*Transactional Information Flow Control SFP*] based on the following types of subject and information security attributes:

[

End User (subject) attributes:

a. User name
b. Personal security image and caption
c. Challenge questions/answers
d. Out-of-Band authentication information
e. Network information
f. Device information

Transactional (information) attributes:

a. Risk factor

].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[

a. (In "Transactional Authentication" deployment) The End User is deemed valid, and risk analysis by the TOE Risk and Policy Engine has determined that the transaction can proceed
b. (In "Transactional Monitoring" deployment) No rules

].

FDP_IFF.1.3

The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1

The TSF shall enforce the [*Back Office User Access Control SFP and End User Access SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*no additional importation control rules*].

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

6.2.3 Class FIA: Identification and Authentication

FIA_ATD.1(a) User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1(a)

The TSF shall maintain the following list of security attributes belonging to individual **Back Office** users:
[
a. *User name*
b. *Password*
c. *Assigned Back Office Tool(s)*
d. *Assigned Role*
e. *Assigned Operations*
].

Dependencies: No dependencies

FIA_ATD.1(b) User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1(b)

The TSF shall maintain the following list of security attributes belonging to individual **End** users:
[
a. *User name*
b. *Personal security image*
c. *Challenge question(s) and answer(s)*
d. *Out-of-Band Challenge information*
e. *Network information (IP address, etc.)*
f. *Device information*
].

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1

The TSF shall provide a mechanism to verify that **Back Office User passwords** ~~secrets~~ meet [*the minimum length requirement of eight (8) characters*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
FIA_UAU.1.1

The TSF shall allow
[
Access to the TOE's Adaptive Authentication Utilities component, which includes the following utilities:
a. *Aggregator Token Generator*
b. *Billing Utility*
c. *Configuration Framework*
d. *eFraudNetwork Agent and Database Loader*
e. *GeoIP Admin Tool and Inspector Utility*
f. *HealthCheck Servlet*
g. *LogManager Servlet*
]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each **Back Office** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **Back Office** user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each **End** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide [*challenge questions and out-of-band challenges*] to support **End** user authentication.

FIA_UAU.5.2

The TSF shall authenticate any **End** user's claimed identity according to the [*challenge question and out-of-band challenge rules for responses and timing*].

Dependencies: No dependencies

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1

The TSF shall re-authenticate the **End** user under the conditions [*the TOE Risk and Policy Engine determines that the risk factor associated with a given transaction is high enough to warrant the submission of additional authentication credentials, based on the End User Access Control SFP*].

Dependencies: No dependencies

Application Note: The End User Access Control SFP is defined in FDP_ACC.1(b) and FDP_ACF.1(b).

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1

The TSF shall provide only [*replacement symbols for characters during password entry*] to the **Back Office** user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow

[

Access to the TOE's Adaptive Authentication Utilities component, which includes the following utilities:

a. Aggregator Token Generator
b. Billing Utility
c. Configuration Framework
d. eFraudNetwork Agent and Database Loader
e. GeoIP Admin Tool and Inspector Utility
f. HealthCheck Servlet
g. LogManager Servlet

]
on behalf of the **Back Office** user to be performed before the **Back Office** user is identified.

FIA_UID.1.2

The TSF shall require each **Back Office** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that **Back Office** user.

Dependencies: No dependencies

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each **End** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MOF.1(a) Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1(a)
The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*available via the TOE Back Office Tools utilities*] to [*the "admin" role*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1(b) Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1(b)
The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*available via the TOE Back Office Tools Policy Editor utility*] to [*the "editor" role*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(a) Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1(a)
The TSF shall enforce the [*Back Office User Access Control SFP*] to restrict the ability to [query, modify] the security attributes [*associated with Back Office users, Transactional Information Flow Control SFP, and cases*] to [*"admin" role users*].
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(b) Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1(b)
The TSF shall enforce the [*Back Office User Access Control SFP*] to restrict the ability to [query, modify] the security attributes [*associated with the Transactional Information Flow Control SFP*] to [*"editor" role users*].
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(c) Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1(c)
The TSF shall enforce the [*Back Office Access Control SFP*] to restrict the ability to [query] the security attributes [*associated with the Transactional Information Flow Control SPF*] to [*"reviewer" role users*].
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Back Office Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*"admin" role users*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1(a) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(a)

The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*Back Office User, Transactional Information Flow Control SFP, and case data*] to [*the "admin" role*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1(b) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(b)

The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*Transactional Information Flow Control SFP data*] to [*the "editor" role*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1(c) Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1(c)

The TSF shall restrict the ability to [query] the [*Transactional Information Flow Control SFP data*] to [*the "reviewer" role*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

[

a. *Management of security functions behaviour*
b. *Management of security attributes*
c. *Management of TSF data*

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*"admin", "editor", "reviewer", and "fraudanalyst"*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class EXT_FCR: Case Recording and Review

EXT_FCR_ARP.1 Security alarms
Hierarchical to: No other components
EXT_FCR_ARP.1.1
The TSF shall make the recommendation [*allow, deny, monitor, challenge, review*] upon determination of a heightened potential of risk for a given transaction.
Dependencies: EXT_FCR_CDA.1 Potential violation analysis

EXT_FCR_GEN.1 Case data generation
Hierarchical to: No other components
EXT_FCR_GEN.1.1
The TSF shall be able to generate case data of the following monitored activities:
[
a. *High-risk user activities in which the recommendation for challenges for additional authentication was made;*
b. *High-risk user activities in which the recommendation for review was made; and*
c. *Manual flagging of an activity by an authorized TOE administrator.*
].
EXT_FCR_GEN.1.2
The TSF shall record within each record at least the following information:
[
a. *User information (including user ID, organization, and authentication status)*
b. *Case information (including case, status resolution, risk score, assigned reviewer)*
c. *Case history*
d. *Recent events*
].
Dependencies: No dependencies

EXT_FCR_CDA.1 Potential violation analysis
Hierarchical to: No other components.
EXT_FCR_CDA.1.1
The TSF shall be able to apply a set of rules in monitoring on-going transactions and, based upon these rules, indicate a potentially fraudulent activity against the TOE-protected system.
EXT_FCR_CDA.1.2.
The TSF shall enforce the following rules for monitoring on-going transactions:
a. Risk factor calculation based on user, device, and transaction data;
b. No other rules.
Dependencies: EXT_FCR_GEN.1 Case data generation

EXT_FCR_CDA.2 Simple attack heuristics
Hierarchical to: EXT_FCR_CDA.1 Potential violation analysis
EXT_FCR_CDA.2.1
The TSF shall be able to maintain an internal representation of the following risk information: [*country or IP blacklists, watch lists, and "white" lists*] that help in determining a level of risk for a given transaction.
EXT_FCR_CDA.2.2

The TSF shall be able to compare the stored risk information against information about the current transaction discernible from an examination of

[

a. *Client machine information*
b. *Browser information*
c. *IP address, IP profile, and geoIP information*
d. *User device history information*
e. *User profile and behavior*
f. *Transaction information*

].

EXT_FCR_CDA.2.3

The TSF shall be able to indicate an appropriate course of action for a given transaction when the level of risk for a transaction indicates a potentially fraudulent use of a TOE-protected system.

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 14 - Assurance Requirements summarizes the requirements.

Table 14 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM[24] system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[24] CM – Configuration Management

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 15 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1(a)	Subset access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
Identification and Authentication	FIA_ATD.1(a)	User attribute definition
	FIA_ATD.1(b)	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.6	Re-authenticating
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
	FIA_UID.2	User identification before any action

TOE Security Function	SFR ID	Description
Security Management	FMT_MOF.1(a)	Management of security functions behaviour
	FMT_MOF.1(b)	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.1(c)	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1(a)	Management of TSF data
	FMT_MTD.1(b)	Management of TSF data
	FMT_MTD.1(c)	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Case Recording and Review	EXT_FCR_ARP.1	Security alarms
	EXT_FCR_GEN.1	Case data generation
	EXT_FCR_CDA.1	Potential violation analysis
	EXT_FCR_CDA.2	Simple attack heuristics

7.1.1 Cryptographic Support

The TOE provides encryption of End User credentials, including answers to secret challenge questions and site-to-user phrases encrypted in the databases. The TOE also encrypts cookies used to bind a user to a device, as well as Authentication Credential Service Provider (ACSP) session data for Out-Of-Band (OOB) authentication. The Back Office applications use hashing functionality for password management and not encryption. The cryptographic functionality is provided by a FIPS 140-2-validated cryptographic module: RSA BSAFE Crypto-J JCE Provider Module v4.0, certificate #1048.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.2 User Data Protection

The RSA Adaptive Authentication System v6.0.2.1 with Service Pack 3 provides an authentication mechanism for controlling access to Back Office administrative functions of the TOE. This mechanism ensures that access to administrative functions and data is available (but restricted to) authorized administrators only.

End Users' access to the TOE, while indirect, is primarily controlled by the front-end application. However, the TOE adds another layer of authentication based on additional factors (such as positive device identification). This access control mechanism ensures that access to protected data is granted only as permitted by policy.

Further, the TOE also provides for the definition of risk-based policies that require End Users to provide credentials in order to perform transactions under certain policy-controlled conditions. This mechanism

ensures that potentially fraudulent transactions on End User data are monitored, the front-end applications are notified, and recommendations for further action are made when appropriate.

Back Office User credentials, End User credentials, transaction data, risk data, and other data are stored by the TOE in the external database. This data is stored and retrieved without security attributes and processed by the TOE upon import.

7.1.2.1 Back Office User Access Control

The TOE includes a robust set of administrative applications that make up its Back Office Tools set. These tools are used by TOE administrators for configuring and managing cases, reports, and transaction policies. The Access Management tool provides a single interface for access to the other tools in the suite, and allows administrators to create and manage users and user permissions for these applications.

Each user is created with the following associated data:

- Name
- Organization
- Assigned Back Office Tool(s)
- Assigned Role(s)
- Assigned Operation(s)

Within the TOE, the Role defines the operations, or permissions, that the user can exercise within the assigned Back Office Tools. Each Role can be assigned one or more of the following operations: CREATE, READ, UPDATE, and DELETE.

Access to the Back Office tools (and the operations allowed while using those tools) requires having the appropriate credentials and permissions. Without them, access is denied.

7.1.2.2 End User Access Control

End users do not directly interface with the TOE. Instead, requests are made by a host application on behalf of the user.

Authentication requests are made to the host application. Once the host application determines if the user is valid, the host application then ascertains if the user is "enrolled" in the RSA AA System. If not, the user is given the opportunity to enroll at that time.

The host application then collects the necessary information and passes it to the TOE. The TOE uses this information to determine a recommended action based on its stored policies. The recommendation will either be ALLOW, CHALLENGE, REVIEW, or DENY.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1.

7.1.3 Identification and Authentication

7.1.3.1 Back Office User Authentication

TOE administrators (i.e. Back Office users) are identified by a user name, and are authenticated by a password. Back Office users log in to the Access Management interface by entering their user name/password combination. The system creates four users by default: admin, editor, fraudanalyst, and reviewer. These users cannot be removed from the system.

The passwords used by Back Office users must fulfill minimum strength requirements, such that passwords must be at least eight characters in length. Password characters will be replaced by symbols during password entry to prevent reading of the password.

Back Office users may only access the TOE Adaptive Authentication Utilities prior to identifying and authenticating to the TOE:

7.1.3.2 End User Authentication

End users must authenticate to the host application each time they wish to perform an activity (sign-in or transaction) that is defined as risky within the host application. An End User may not perform any actions on the TOE prior to identifying and authenticating.

For the initial login, the End user must provide whatever information is required by that system, often a user name/password combination. However, once the host application has determined that the credentials are valid, further device and network information is collected and passed to the TOE to determine the risk factor. From this point, the "sign-in" process can take any one of three paths depending on the TOE deployment mode.

- Sign-in with Risk-Based Authentication mode – When deployed in this mode, the TOE will authenticate End Users based on factors such as their network information, user information, positive device identification, and user profiling. All of these factors are fed to the TOE Risk and Policy Engine, which then makes a determination of risk. Users with high risk are challenged (the TOE recommends that the host application require further proof of identity), while users with low risk are allowed to continue.

- Sign-in with Positive Device Identification Only mode – When deployed in this mode, the TOE will authenticate End users based primarily on device binding. The TOE checks to see if it recognizes the device from which the user is logging into the host application. It looks at a large number of device characteristics to uniquely identify the user's device, and determines a risk based on its recognizing of the device. Again, users with high risk are challenged, while users with low risk are allowed to continue.

- Sign-in Monitoring mode – When deployed in this mode, the TOE performs a risk analysis just as it does in the other deployment modes. However, no recommendations are made based on that risk; all users are allowed to continue, while potentially risky logins are simply flagged for later review.

Challenges take the form of challenge questions or out-of-band (OOB) challenges. Challenge questions require the user to respond to a previously-selected question, and the user response will be compared to their stored answer for correctness. OOB challenges require the user to type a one-time password (presented on their web page) on their phone keypad.

7.1.3.3 Transaction Authentication and Monitoring

End user transactions can also result in challenges. A risk factor for each transaction is calculated by the TOE Risk and Policy Engine. If the TOE is deployed in Transactional Authentication mode and if the risk factor for a particular transaction is high, then the End user will be challenged for more credentials. The challenge process for transactions works the same as it does for logins. If the TOE is deployed in Transactional Monitoring mode then all transactions are monitored but no further authentication challenges are issued to the user.

TOE Security Functional Requirements Satisfied: FIA_ATD.1(a), FIA_ATD.1(b), FIA_SOS.1, FIA_UAU.1, FIA_UAU.2 FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.1, FIA_UID.2.

7.1.4 Security Management

The TOE is managed by administrators (Back Office Users) who have varying degrees of authority to review and modify the configuration of the security attributes of the TOE. Levels of administrative authority are based on the credentials used to authenticate. Back Office Users have associated modules (accessible Back Office tools) and roles (predefined sets of permissions). While administrators can create roles, the TOE comes pre-populated with the following roles that can perform security management tasks:

- admin – this role is a "super-user" that can has all permissions (CREATE, READ, UPDATE, DELETE)
- editor – this role can make changes in the Policy Editor (CREATE, READ, UPDATE, DELETE)
- reviewer – this role can review policies (READ)
- fraudanalyst – this role is only assigned to the fraudanalyst user, and is used to query the TOE database for cases that may have fraudulent activity (READ).

Along with these predefined roles, the TOE has several users predefined as well. For ease of association, the names of the users match their roles. They are "admin", "editor", "reviewer", and "fraudanalyst". These users cannot be deleted, and are configured with default passwords. It is recommended that the passwords be changed.

Back Office users with the proper credentials can also administer both users and roles. Using the Access Management tool, administrators can create a user, remove a user (excluding the system-defined default users), and modify user details, including their module(s) and role(s). Administrators can also create, edit, and remove roles. This feature gives administrators the capability to configure roles and users specifically for their own business needs and concerns.

While the TOE comes equipped with default policies, administrators can add, delete, or alter policies to fit their specific requirements. Using the Policy Editor, Back Office users can configure and customize the necessary policies by which the TOE detects and challenges potentially risky End users and transactions. Depending on the TOE deployment, events of a sufficient risk level can be recorded in a case log for later evaluation.

TOE Security Functional Requirements Satisfied: FMT_MOF.1(a), FMT_MOF.1(b), FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.3, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(c), FMT_SMF.1, FMT_SMR.1.

7.1.5 Case Recording and Review

The TOE's primary function is to detect and react to potentially fraudulent activities against a system it is configured to protect. This is accomplished via the monitoring of End User transactions as they occur. Each transaction is analyzed for its potential risk, and policy-based recommendations are made to the host application based on the risk value determined by the TOE. The TOE continuously monitors the End User transactions and can record information about questionable logins and transaction request for later review.

TOE Security Functional Requirements Satisfied: EXT_FCR_ARP.1, EXT_FCR_GEN.1, EXT_FCR_CDA.1, EXT_FCR_CDA.2.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

There are no Protection Profile conformance claims associated with this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DOS An attacker may attempt to flood the TOE with network traffic, rendering the TOE's services inaccessible to authorized users.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK ensures that the environment provides a network configuration capable of protecting against denial-of-service and other network-based attacks, which would prevent the TOE from carrying out its intended functions.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the environment provides protection for the TOE from outside interference.
T.FRAUD An attacker may take advantage of weak authentication mechanisms to commit fraudulent activities against the host application employing the TOE.	O.ENDUSER_AUTH The TOE must be able to identify and authenticate end users prior to allowing access to end user functions and data and high-risk transactions.	O.ENDUSER_AUTH ensures that access to TOE-protected data is restricted to authenticated users only.
	O.MONITOR The TOE must provide a mechanism to continuously monitor end user transactions, and to record potentially risky transactions for later review.	O. MONITOR ensures that transactions occurring on a TOE-protected host application can be monitored and recorded for later inspection.
	O.RECOMMEND The TOE must be able to make recommendations regarding the submission of authentication	O. RECOMMEND ensures that the TOE is equipped with a mechanism for determining the risk involved with a given

Threats	Objectives	Rationale
	credentials based on a calculated risk associated with the login attempt or transaction.	transaction, and make a recommendation based on that risk whether the host application should allow a potentially-fraudulent transaction to occur.
	OE.SECURE_COMMS The TOE environment must ensure that communications between the TOE components, the database server, front-end applications, and the RSA Data Center are protected via a secure channel.	OE.SECURE_COMMS ensures that communications between the TOE and non-TOE support systems are protected from tampering and eaves-dropping.
T.MASQUERADE An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.ADMIN_AUTH The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.	O. ADMIN_AUTH mitigates this threat by ensuring that the TOE identifies and authenticates users prior to allowing access to TOE administrative functions and data.
	O.ENDUSER_AUTH The TOE must be able to identify and authenticate end users prior to allowing access to end user functions and data and high-risk transactions.	O.ENDUSER_AUTH ensures that access to TOE-protected data is restricted to authenticated users only.
T.TAMPERING An attacker may be able to bypass the TOE's security mechanisms by tampering with the TOE or the TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
	OE.SECURE_COMMS The TOE environment must ensure that communications between the TOE components, the database server, front-end applications, and the RSA Data Center are protected via a secure channel.	OE.SECURE_COMMS ensures that communications between the TOE and non-TOE support systems are protected from tampering.
T.UNAUTH An attacker may gain access to	O.ADMIN The TOE must include a set of	O.ADMIN ensures that access to TOE security data is limited to

Threats	Objectives	Rationale
security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.	those users with access to the management functions of the TOE.
	O.ADMIN_AUTH The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.	O.ADMIN_AUTH ensures that administrators are identified and authenticated prior to gaining access to TOE security data.
	O.VALIDATED_CRYPTO The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 cryptographic module.	O.VALIDATED_CRYPTO ensures that the TOE provides cryptographic functionality such as encryption and certificate authentication, ensuring that data that is stored on the TOE, or transmitted through the TOE or between the TOE and an external device cannot be accessed.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 17 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.ADMIN The TOE shall provide a set of tools for the secure management of TOE data and functions.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.	O.ADMIN ensures that TOE management tools are available for (and restricted for) use by TOE administrators.
P.CASELOG The TOE shall have the capability to record "high-risk" events and activities in a case log for later review.	O.MONITOR The TOE must provide a mechanism to continuously monitor end user transactions, and to record potentially risky transactions for later review.	O.MONITOR provides the ability to monitor and record potentially-fraudulent transactions to a specified location, such that a fraud analyst could review said information.

Policies	Objectives	Rationale
P.INTEGRITY Data collected and produced by the TOE shall be protected from unauthorized deletion or modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE environment provided a mechanism to protect itself from outside tampering and interference, minimizing the threat of tampering with TOE data.
P.MANAGE The TOE shall only be managed by authorized users.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.	O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
P.RECOMMEND The TOE shall make recommendations regarding the submission of authentication credentials based on a calculated risk associated with the login attempt or transaction.	O.RECOMMEND The TOE must be able to make recommendations regarding the submission of authentication credentials based on a calculated risk associated with the login attempt or transaction.	O.RECOMMEND ensures that the TOE can recommend a course of action based on its risk factor determination and risk analysis.
P.RISK The TOE shall have the capability to compute a "risk factor" for a given end user login attempt or transaction.	O.RISK_FACTOR The TOE must provide a mechanism for determining a "risk factor" of allowing a given login or transaction to be performed.	O. RISK_FACTOR ensures that the TOE has a means for determining and providing a risk factor for a specified end user event.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.AUDIT The operating system that the TOE is installed on is correctly configured by the administrator to audit all administrative actions that the administrator deems necessary.	OE.AUDIT The TOE environment will be configured to audit all administrative actions.	OE.AUDIT ensures that all TOE administrative actions (deemed important by the administrator) are audited by the underlying Operating System.
A.INSTALL The TOE is properly installed on a hardware and operating system capable of supporting all of its	OE.PLATFORM The TOE hardware and Operating System must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and Operating System supports the TOE functions.

Assumptions	Objectives	Rationale
required functionality.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE ensures that TOE administrators are capable for performing a TOE installation on the proper platform.
A.LOCATE The TOE is located within a controlled access facility	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE environment provides protection for the TOE from unauthorized access.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL ensures that the physical security provided by the TOE environment provides appropriate protection to the TOE by controlling access to the facility.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NETCON The TOE environment provides a private network that allows the TOE to provide its security functions to TOE components, the database server, front-end applications, and the RSA Data Center.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
	OE.PLATFORM The TOE hardware and Operating System must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and Operating System supports the TOE functions.
	OE.SECURE_COMMS The TOE environment must ensure that communications between the TOE components, the database server, front-end applications, and the RSA Data Center are protected via a secure channel.	OE.SECURE_COMMS ensures that communications between the TOE and non-TOE support systems are protected from tampering and eaves-dropping.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are	NOE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow

Assumptions	Objectives	Rationale
	appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	all guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT satisfies this assumption that the TOE environment will provide protection from external interference or tampering.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A class of EXT_FCR requirements was created to specifically address the capability of the TOE to monitor transactions and record transaction data that represents potentially fraudulent activity against a TOE-protected system. The FAU: Security Audit class was used as a model for creating these requirements. The purpose of this class of requirements is to define the security functionality provided by the end user transaction monitoring of the TOE. There are no existing CC SFRs that can be used to appropriately describe this functionality, so the extended components were created with wording that adequately captures the functionality being claimed. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE Security Assurance components associated with this evaluation.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 19 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient	FMT_MOF.1(a) Management of security functions behaviour	This requirement meets the objective O.ADMIN by providing functions to manage TOE security

Objective	Requirements Addressing the Objective	Rationale
management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, may exercise such management control.		functions, and by ensuring that the management of the functions' behavior is restricted to authorized users only.
	FMT_MOF.1(b) Management of security functions behaviour	This requirement meets the objective O.ADMIN by providing functions to manage TOE security functions, and by ensuring that the management of the functions' behavior is restricted to authorized users only.
	FMT_MSA.1(a) Management of security attributes	This requirement meets the objective O.ADMIN by providing functions to manage TOE security attributes, and by ensuring that the management of the attributes is restricted to authorized users only.
	FMT_MSA.1(b) Management of security attributes	This requirement meets the objective O.ADMIN by providing functions to manage TOE security attributes, and by ensuring that the management of the attributes is restricted to authorized users only.
	FMT_MSA.1(c) Management of security attributes	This requirement meets the objective O.ADMIN by providing functions to manage TOE security attributes, and by ensuring that the management of the attributes is restricted to authorized users only.
	FMT_MSA.3 Static attribute initialisation	This requirement meets the objective by providing a function to manage default values for given security attributes, and by restricting that capability to authorized users.
	FMT_MTD.1(a) Management of TSF data	This requirement meets the objective O.ADMIN by providing functions to manage TSF data, and by ensuring that the management of the data is restricted to authorized users only.
	FMT_MTD.1(b) Management of TSF data	This requirement meets the objective O.ADMIN by providing functions to manage TSF data, and by ensuring that the management

Objective	Requirements Addressing the Objective	Rationale
		of the data is restricted to authorized users only.
	FMT_MTD.1(c) Management of TSF data	This requirement meets the objective O.ADMIN by providing functions to manage TSF data, and by ensuring that the management of the data is restricted to authorized users only.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective O.ADMIN by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective O.ADMIN by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ADMIN_AUTH The TOE must be able to identify and authenticate administrative users prior to allowing access to TOE administrative functions and data.	FDP_ACC.1(a) Subset access control	The requirement meets the objective O.ADMIN_AUTH by ensuring that access control is applied to users before they are allowed access to TOE administrative functions and data.
	FDP_ACF.1(a) Security attribute based access control	The requirement meets the objective O.ADMIN_AUTH by ensuring that the TOE enforces access control based on the implemented policy.
	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective O.ADMIN_AUTH by ensuring that administrative user credentials are stored in the external database.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective O.ADMIN_AUTH by ensuring that administrative user credentials are retrieved from the external database.
	FIA_ATD.1(a) User attribute definition	The requirement meets the objective O.ADMIN_AUTH by maintaining a set of security attributes used for administrators to authenticate.
	FIA_SOS.1	The requirement meets the

Objective	Requirements Addressing the Objective	Rationale
	Verification of secrets	objective O.ADMIN_AUTH by ensuring that administrator passwords meet a minimum length criterion.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective O.ADMIN_AUTH by ensuring that administrators cannot perform TSF-mediated functions before authenticating to the TOE.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective O.ADMIN_AUTH by ensuring that limited feedback is given while administrators authenticate to the TOE.
	FIA_UID.1 Timing of identification	The requirement meets the objective O.ADMIN_AUTH by ensuring that administrators cannot perform TSF-mediated functions before being identified by the TOE.
	FMT_MOF.1(a) Management of security functions behaviour	The requirement meets the objective O.ADMIN_AUTH by ensuring that TOE security functions can be managed only by authorized administrators.
	FMT_MOF.1(b) Management of security functions behaviour	The requirement meets the objective O.ADMIN_AUTH by ensuring that TOE security functions can be managed only by authorized administrators.
	FMT_MSA.1(a) Management of security attributes	The requirement meets the objective O.ADMIN_AUTH by ensuring that security attributes can be managed only by authorized administrators.
	FMT_MSA.1(b) Management of security attributes	The requirement meets the objective O.ADMIN_AUTH by ensuring that security attributes can be managed only by authorized administrators.
	FMT_MSA.1(c) Management of security attributes	The requirement meets the objective O.ADMIN_AUTH by ensuring that security attributes can be managed only by authorized administrators.
	FMT_MSA.3	This requirement meets the

Objective	Requirements Addressing the Objective	Rationale
	Static attribute initialisation	objective by restricting the capability to manage default values for given security attributes to authorized administrators.
	FMT_MTD.1(a) Management of TSF data	The requirement meets the objective O.ADMIN_AUTH by ensuring that TSF data can be managed only by authorized administrators.
	FMT_MTD.1(b) Management of TSF data	The requirement meets the objective O.ADMIN_AUTH by ensuring that TSF data can be managed only by authorized administrators.
	FMT_MTD.1(c) Management of TSF data	The requirement meets the objective O.ADMIN_AUTH by ensuring that TSF data can be managed only by authorized administrators.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective O.ADMIN_AUTH by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective O.ADMIN_AUTH by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ENDUSER_AUTH The TOE must be able to identify and authenticate end users prior to allowing access to end user functions and data and high-risk transactions.	FDP_ACC.1(b) Subset access control	The requirement meets the objective O.ENDUSER _AUTH by ensuring that access control is applied to end users before they are allowed access to user functions and data.
	FDP_ACF.1(b) Security attribute based access control	The requirement meets the objective O.ENDUSER _AUTH by ensuring that the TOE enforces access control based on the implemented policy.
	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective O.ENDUSER_AUTH by ensuring that end user credentials are stored in the external database.

Objective	Requirements Addressing the Objective	Rationale
	FDP_IFC.1 Subset information flow control	The requirement meets the objective O.ENDUSER _AUTH by requiring that end users authenticate before being given access to transaction-related functions and data.
	FDP_IFF.1 Simple security attributes	The requirement meets the objective O.ENDUSER _AUTH by enforcing information flow control policies based on end user authentication data.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective O.ENDUSER_AUTH by ensuring that end user credentials are retrieved from the external database.
	FIA_ATD.1(b) User attribute definition	The requirement meets the objective O.ENDUSER _AUTH by defining the attributes by which end users are authenticated.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective O.ENDUSER _AUTH by ensuring that end users are authenticated before access to TSF-mediated functions is allowed.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective O.ENDUSER _AUTH by providing multiple methods for End Users to provide additional credentials when required.
	FIA_UAU.6 Re-authenticating	The requirement meets the objective O.ENDUSER _AUTH by ensuring that End Users re-authenticate as required by the information flow control policy.
	FIA_UID.2 User identification before any action	The requirement meets the objective O.ENDUSER _AUTH by ensuring that End Users are identified before access to TSF-mediated functions is allowed.
O.MONITOR The TOE must provide a mechanism to continuously monitor end user transactions, and to record potentially risky transactions for later review.	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective O.MONITOR by ensuring that transaction data is stored in the external database.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective O.MONITOR by ensuring that transaction data is

Objective	Requirements Addressing the Objective	Rationale
		retrieved from the external database.
	EXT_FCR_GEN.1 Case data generation	This requirement meets the objective O.MONITOR by defining which monitored activities result in case data, as well as what data must be recorded.
	EXT_FCR_CDA.1 Potential violation analysis	This requirement meets the objective O.MONITOR by ensuring that the detection of potentially fraudulent activities relies on the monitoring of on-going transactions.
O.RECOMMEND The TOE must be able to make recommendations regarding the submission of authentication credentials based on a calculated risk associated with the login attempt or transaction.	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective O.RECOMMEND by ensuring that risk data is stored in the external database.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective O.RECOMMEND by ensuring that risk data is retrieved from the external database.
	EXT_FCR_CDA.2 Simple attack heuristics	This requirement meets the objective O.RECOMMEND by providing a mechanism to determine the risk involved with a given transaction, and the ability to recommend a course of action based on that risk factor.
O.RISK_FACTOR The TOE must provide a mechanism for determining a "risk factor" of allowing a given login or transaction to be performed.	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective O.RISK_FACTOR by ensuring that risk data is stored in the external database.
	FDP_ITC.1 Import of user data without security attributes	The requirement meets the objective O.RISK_FACTOR by ensuring that risk data is retrieved from the external database.
	EXT_FCR_ARP.1 Security alarms	This requirements meets the objective O.RISK_FACTOR by requiring that a recommendation for action be made based on a risk factor determined by the TOE.
	EXT_FCR_CDA.1 Potential violation analysis	This requirement meets the objective O.RISK_FACTOR by ensuring that the detection of potentially fraudulent activities relies on the calculation of a risk

Objective	Requirements Addressing the Objective	Rationale
		factor.
O.VALIDATED_CRYPTO The TOE shall provide cryptographic functions for its own use. These functions will be provided by a FIPS 140-2 cryptographic module.	FCS_CKM.1 Cryptographic key generation	This requirement supports O.VALIDATED_CRYPTO by providing cryptographic key generation, which can be used to ensure cryptographic functionality on the TOE.
	FCS_CKM.4 Cryptographic key destruction	This requirement supports O.VALIDATED_CRYPTO by providing a method for destroying cryptographic keys, thereby ensuring that the keys are not accessed by an unauthorized person or IT entity.
	FCS_COP.1 Cryptographic operation	This requirement supports O.VALIDATED_CRYPTO by providing algorithms for cryptographic operation, which can be used to encrypt and decrypt data passing through or being stored on the TOE, or data passing between the TOE and an external device.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 20 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(a)	FMT_MSA.3	✓	
	FDP_ACC.1(a)	✓	
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
	FMT_MSA.3	✓	
FDP_ETC.1	FDP_ACC.1(b)	✓	
	FDP_ACC.1(a)	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3	✓	
	FDP_IFC.1	✓	
FDP_ITC.1	FDP_ACC.1(a)	✓	
	FMT_MSA.3	✓	
	FDP_ACC.1(b)	✓	
FIA_ATD.1(a)	No dependencies		
FIA_ATD.1(b)	No dependencies		
FIA_SOS.1	No dependencies		
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.2	FIA_UID.1	✓	
FIA_UAU.5	No dependencies		
FIA_UAU.6	No dependencies		
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	No dependencies		
FIA_UID.2	No dependencies		
FMT_MOF.1(a)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MOF.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.1(a)	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1(a)	✓	
FMT_MSA.1(b)	FDP_IFC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1(a)	✓	
FMT_MSA.1(c)	FMT_SMR.1	✓	
	FDP_IFC.1	✓	
	FDP_ACC.1(a)	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1(a)	✓	
FMT_MTD.1(a)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1(b)	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1(c)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	
EXT_FCR_ARP.1	EXT_FCR_CDA.1	✓	
EXT_FCR_GEN.1	No dependencies		
EXT_FCR_CDA.1	EXT_FCR_GEN.1	✓	
EXT_FCR_CDA.2	EXT_FCR_GEN.1	✓	

9 Acronyms

This section defines the acronyms used in this document.

9.1 Acronyms

Table 21 - Acronyms

Acronym	Definition
AA	Adaptive Authentication
ACSP	Authentication Credential Service Provider
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher-Block Chaining
CC	Common Criteria
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CM	Configuration Management
CSR	Customer Service Representative
CTR	Counter
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP	Internet Protocol
IT	Information Technology
MAC	Message Authentication Code
OFB	Output Feedback
OOB	Out-Of-Band
OSP	Organizational Security Policy

Acronym	Definition
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
RSA	Rivest, Shamir, and Adleman
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Triple Data Encryption Standard
TSF	TOE Security Functionality
VXML	Voice Extensible Markup Language
WSDL	Web Services Description Lanaguage

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com