Certification Report

EAL 4+ (ALC_FLR.1) Evaluation of

RioRey, Incorporated
RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	13.03.2013
Version of Report	1.0
Author	Mehmet Kürşad ÜNAL
Technical Responsible	Mustafa YILMAZ
Approved	Mariye Umay AKKAYA
Date Approved	13.03.2013
Certification Number	14.10.06/13-006
Sponsor and Developer	RioRey, Incorporated
Evaluation Lab	CygnaCom Solutions, Inc
TOE	RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9
Pages	14

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
v1.0	13.03.2013	All	Final Released

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document have been evaluated at an accredited and licensed evaluation facility conformant to Common Criteria for IT Security Evaluation, version 3.1, revision 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit to the Certification Committee the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. The Certification Report covers all non-confidential security and technical information related to a Common Criteria evaluation, which is made under the PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCCS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCEF) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations, which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by CygnaCom Solutions, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product, and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9, whose evaluation was completed on 25.10.2012 and whose evaluation technical report was drawn up by CygnaCom (as CCTL), and with the Security Target document version 0.9 of the relevant product.

The certification report, certificate of product evaluation, and security target document are posted on the PCC Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: RioRey™ Perimeter Protection Platform Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9

Developer's Name: RioRey Incorporated

Name of CCTL: CygnaCom Solutions, Inc

Assurance Package: EAL 4+(ALC_FLR.1)

Completion Date of Evaluation: 25.10.2012

TOE major security features for operational use:

Audit generation: The TOE generates audit data such as the system log, traffic alarm summary, system alarm events, victim information, attacker history…etc.

Audit protection: The TSF protects the stored audit records on the TOE from unauthorized deletion and modifications via the TSFI. The TSF retains log files on the local system (System Information and Attack Information).

Audit review: An authorized user can read all audit data generated.

Selectable Audit Review: The TSF is able to perform searches and sorting of stored audit data based on various criteria and logical relations specified by an authorized administrator.

Resource Utilization: The TOE uses three notions of lists which are black, white, and filter. Any packets not matching any Black or Filter lists are allowed through and any packets matching a White list are allowed through the Platform.

DDoS Protection Mechanisms: The TOE performs a lot of tests for the incoming packets. These test are:

- Spoofed IP Test
- Responsiveness Test
- Fragmentation Test
- Payload Randomness Test
- TCP Session Checker Test
- TCP Regex Checker Test
- TCP Port Usage Conformance Test
- TCP Application Layer Analysis Test
- Other Tests

DDoS Information Flow Control Capabilities: The TOE has various information flow control capabilities. These are:

- Filter, Monitor or Bypass modes
- Traffic Control Based on Whitelist Specifications
- Traffic Control Based on Blacklist Specifications
- Service Definitions
- Fragmentation Control
- TCP SYN Rate Configuration

Failure with Preservation of Secure State: Secure state for this product is defined as the state when the TOE platform provides uninterrupted access to resources on the internal network to intended users. There are 3 types of failures. These are Hardware, power and software failures.

Basic Internal TSF data transfer protection: The rView Software connects to the Platform using the standard SSH-2 protocol through OpenSSH version 5.1p1 which provides confidentiality and integrity of data over an insecure network. The PC that runs rView must therefore be on a network where TCP Port 8022 access is enabled to the Platform Management Port.

User Attributes: Username, password and role assignment are maintained by the TSF for each individual TOE user for use with local password authentication only.

User Identification and Authentication: The TSF requires each user to self-identify before being allowed to perform any other actions. The TSF requires an administrator to be successfully authenticated with a password before being allowed any other management actions. Authentication is handled via local password protection or the TOE invokes an external authentication mechanism (RADIUS) for the authentication decision.

Management of TSF Data: The allowed operations on TSF Data and the administrative roles required to execute them are defined in the Security Target.

Specification of Management Functions: The TOE is capable of performing the security management functions as defined in the Security Target. All management functions are limited to the administrative roles.

Security Roles: The TOE supports the 3 roles which are Admin, Normal and View only.

The Target of Evaluation (TOE) is a DDoS mitigation appliance with Java application, which is called RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9.

rView is a Java application that allows an administrator to configure and monitor the Platform in real time. The rView software can run on Windows XP, Vista, Windows 7, Linux and MacOSX. The minimum requirements for rView running on Windows machines:

- Windows XP, Vista, Windows 7(all editions)
- 100 MB of free hard disk space
- 1GB of RAM
- Java JRE 1.6 installed on the windows

Minimum requirements for rView running on Linux machines:

- Any major Linux distribution
- 100 MB of free hard disk space
- 1GB of RAM
- Java JRE 1.6 installed on the Linux system
- X-Windows installed on the Linux system

Minimum requirements for rView running on MAC machines:

- OS X 10.5 or higher
- 100 MB of free hard disk space
- 1 GB of RAM
- Java JRE 1.6 installed on the MAC machine

The TOE (RioRey™ solution) provides an integrated hardware and software platform to protect Internet Protocol (IP) networks against DDoS attacks by identifying and filtering attacks while forwarding normal traffic through the network without impacting service.

The Platform recognizes an attack, sends an alert for the threat level it poses and ultimately protects the network from harm rapidly and without operator intervention. RioRey's proprietary technology continuously performs Micro Behavioral Analysis (MBA), looking for distinctive characteristics of network communication. Because RioRey's Perimeter Protection Platforms quickly identify traffic that does not follow normal communication protocols, invalid traffic is immediately blocked. Valid traffic flows are unimpeded and normal network communication is maintained. The hardware and software design is dedicated to this single function. The design is also optimized to tackle high throughput, as well as large numbers of sessions and IP addresses.

An enterprise can deploy multiple RioRey appliances. In such scenarios, the same rView software can be used to manage several appliances individually in the same manner. The TOE does not provide hierarchical management of its appliances.

If a hardware failure occurs and the Platform does not repair itself, the Platform goes into a hardware bypass mode. This connects the WAN and LAN ports, physically bypassing the TOE's filtering mechanisms, maintaining all customer traffic flow through the equipment. An administrator can manually configure the TOE into hardware bypass mode as well. Thus, the DDoS filtering function becomes unavailable, but the flow of traffic is not impeded. In case of a software failure, the multiple watchdogs embedded in the Platform will attempt to restart the Platform and report the incident to the operator. The Platform bypasses customer traffic during the restart phase, maintaining service.

The Platform audits user access events and system processing events (including DDoS attack information) and stores the statistics in RAM for a period of 10 days. The rView Software provides a user friendly way to perform ongoing management of the Platform and obtain Audit information.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	TSE-CCCS-013
TOE Name and Version	RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9
Security Target Document Title	RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series)
Security Target Document Version	0.9
Security Target Date	16.01.2013
Assurance Level	EAL 4+(ALC_FLR.1)
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009

Methodology	Common Methodology for Information Technology Security Evaluation v3.1, rev 3, July 2009
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package Conformant to EAL4+(ALC_FLR.1)
Sponsor and Developer	RioRey, Incorporated
Evaluation Facility	CygnaCom Solutions
Certification Scheme	Turkish Standard Institution Common Criteria Certification Scheme

2.2 Security Policy

The TOE does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

This section describes the assumptions that must be satisfied by the TOE operational environment.

A.CONNECT The TOE will separate the network on which it is installed and operates into external and internal networks. Information cannot flow between the external and internal networks without passing through the TOE.

A.PHYSICAL The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.BACKUP Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.

A.NOEVIL There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The information about the phases mentioned above can be found in the Security Target document.

2.4 Architectural Information

The physical boundary of the TOE is the RE, RX or RG Platform loaded with the RIOS software version 5.0.12sp8 The TOE also includes the rView Software Version 5.0.12sp9. The following figure represents a typical deployment of the RioRey platform.

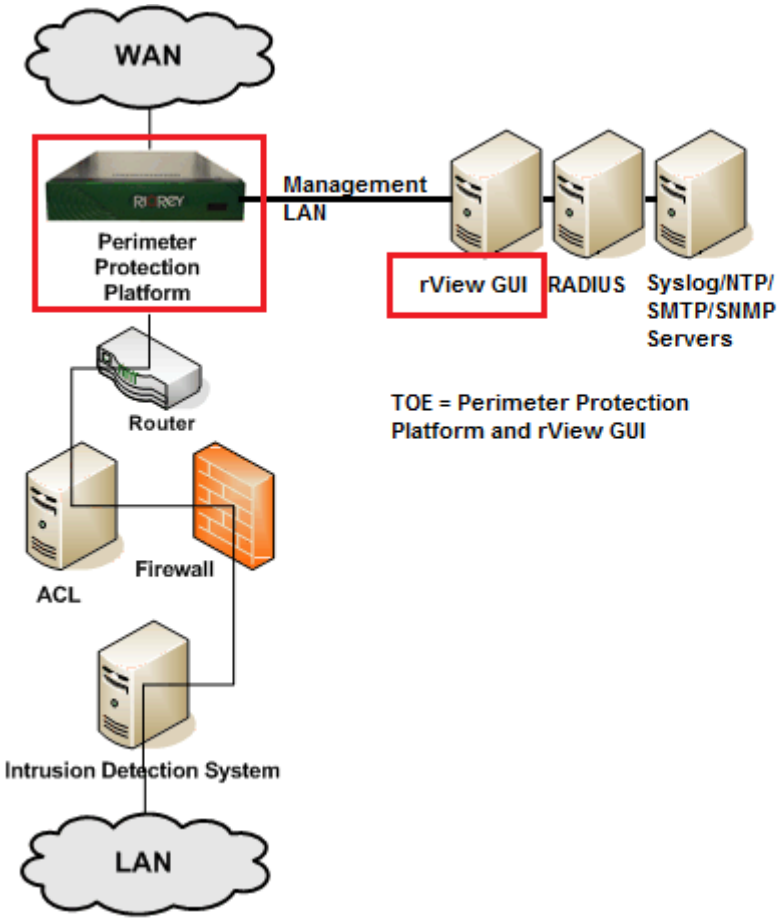

Figure 1: RioRey Deployment

As shown in the first figure, the TOE is Perimeter Protection Platform and rView GUI. The RioRey platform has various models which are RE500, RE1500, RX1800, RX2300, RX4400 and RG Series. These models are available running RIOS software version 5.0.12sp8. rView software is available with version number 5.0.12sp9. The following are included but they are not part of the TOE:

- SNMP browser/Server, SMTP Server, NTP Server, Syslog Server and Web browser are not included in the TOE boundary.
- The system hosting the rView application is also part of the IT Environment.

The following RioRey Products/Services are not included in the scope of evaluation:

- CLI (status, resetpwd, resetip).
- WebUI (deprecated and turned off).

2.5 Documentation

Name of Document	Version Number	Publication Date
RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Security Target	0.9	16.01.2013
CCC_RE_USER_GUIDE_DDSG_V1.2	5.0	-
CCC_RE_USER_GUIDE_SIICG_V1.3	5.0	-
CCC_RG_USER_GUIDE_DDSG_V1.4	5.0	-
CCC_RG_USER_GUIDE_SIICG_V1.5	5.0	-
CCC_RX_USER_GUIDE_DDSG_V1.2	5.0	-
CCC_RX_USER_GUIDE_SIICG_V1.3	5.0	-
RioRey_Version_5_RG.RX.RE_Release_Note_Supplement_V1.4	1.4	October 2012

Table 1

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences - include software, documents, etc - are mapped to the assurance families of Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the Evaluation Technical Report for Target of Evaluation.

It is concluded that the TOE supports EAL 4+ (ALC_FLR.1). There are 25 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

1) Developer Testing:

- **TOE Test Coverage:** Developer has prepared TOE System Test Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE System Test Document according to the TOE design documentation which includes TSF subsystems.
- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results, and actual test results are in the test documentation

2) Evaluator Testing:

- **Independent Testing:** Evaluator has done a total of 63 sample independent tests. 30 of them are selected from developer's test plans. 26 of them are supplemental tests that are provided by the developer to address the lack of tests to cover each type of DDoS attack listed in the .FRU_DDOS_EXT.1 SFR in the Security Target. The other 7 tests are evaluator's independent tests. All of them are related to TOE security functions.
- **Penetration Testing:** Evaluator has done 6 penetration tests to find out if TOE's vulnerabilities can be used for malicious purposes. The potential vulnerabilities are in the evaluation technical report and the results of penetration tests are available in the evaluator test and report document.

The result of AVA_VAN.3 evaluation is given below:

- It is determined that TOE, in its operational environment, is resistant to an attacker

possessing "Enhanced-Basic" attack potential.

- For the product RioRey, **there are no exploitable and/or residual vulnerabilities** in the scope of the assumptions in ST (Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the information it contains and authorized users will not intentionally perform hostile actions).

2.7 Evaluated Configuration

The evaluation's scope includes RE500, RE1500, RX1800, RX2300, RX4400 and RG Series appliances running RIOS software version 5.0.12sp8 and rView Software Version 5.0.12sp9. Under the evaluations the TOE has to provide following conditions:

- Must ensure that the Firewall is enabled and configured on the RioRey™ Perimeter Protection Platform.
- Must ensure that the Firewall IT environment has an NTP server available for the RioRey™ Perimeter Protection Platform to connect to and obtain reliable time.
- Must ensure that the IT environment has an NTP server available for the RioRey™ Perimeter Protection Platform to connect to and obtain reliable time.
- Separate Ethernet Management LAN is established and restricted to management personnel and security supporting IT infrastructure (external authentication server, syslog server, NTP Server, SMTP server, SNMP server, and rView Host. Monitored traffic does not enter or exit this network interface)

2.8 Results of the Evaluation

Table 2 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.1.

Component ID	Component Title
ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance Claims
ASE_SPD.1	Security Problem Definition
ASE_OBJ.2	Security Objectives
ASE_ECD.1	Extended Components Definition
ASE_REQ.2	Derived Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_ARC.1	Security Architecture
ADV_FSP.4	Functional Specification
ADV_IMP.1	Implementation Representation
ADV_TDS.3	TOE Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Configuration Management Capabilities
ALC_CMS.4	Configuration Management Capabilities
ALC_DEL.1	Delivery
ALC_DVS.1	Development Security

ALC_LCD.1	Life-cycle Definition
ALC_TAT.1	Tools and Techniques
ALC_FLR.1	Flaw Remediation
ATE_COV.2	Coverage
ATE_DPT.1	Depth
ATE_FUN.1	Functional Tests
ATE_IND.2	Independent Testing
AVA_VAN.3	Vulnerability Analysis

Table 2

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE (RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9) the results of the assessment of all evaluation tasks are "Pass".

The RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9 product was found to fulfill the Common Criteria requirements for each of 25 assurance families and provide the assurance level EAL 4+ (ALC_FLR.1). This result shows that the TOE is resistant against "Enhanced-Basic" level attack potential and conforms to the claims of the functional and assurance requirements which are defined in the ST document.

There is no residual vulnerability that affects the evaluation result found by CygnaCom laboratory under the conditions defined by the evaluation evidences and developer claims.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9, result of the evaluation, or the ETR.

3 SECURITY TARGET

Information about the Security Target document associated with this certification report is as follows:

Name of Document: RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Security Target Version:0.9 Date: 16.01.2013

Version No.:0.9

Date of Document:16.01.2013

4 GLOSSARY

CCCS:	Common Criteria Certification Scheme
CCTL:	Common Criteria Test Laboratory
CCMB:	Common Criteria Management Board
CEM:	Common Evaluation Methodology
ETR:	Evaluation Technical Report
IT:	Information Technology
PCC:	Product Certification Center
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function
TSFI:	TSF Interface
SFR:	Security Functional Requirement
EAL:	Evaluation Assurance Level
PP:	Protection Profile

5 BIBLIOGRAPHY

[1]Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2]Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3]Common Criteria for Information Technology Security Evaluation, Part 3:Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4]Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3,July 2009

[5]PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS

[6]Evaluation Technical Report for ASE, v3.2, February 11, 2013.

[7]Evaluation Technical Report for a TOE, v2.2, February 28, 2013.

[8] RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Security Target Version:0.9 Date: 16.01.2013

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.