Swedish Certification Body for IT Security

Certification Report - F5 BIG-IP® 14.1.2 VE for LTM+APM

Issue: 1.0, 2020-Nov-04

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a network device. The TOE consists of the BIG-IP LTM+APM Version 14.1.2 (build BIGIP-14.1.2-0.89.37, also referred to as 14.1.2 + EHF) with Appliance Mode licensed, and running on any of the following hypervisors:

- VMWare ESXi 6.5.0 - Intel Xeon E5-2697v4 processor
- Hyper-V version 10.0 on Windows Server 2019 - Intel Xeon E5-2660v3 processor
- KVM on Centos 7 - Intel Xeon E5-2660v3 processor

The hypervisors are installed on the Dell PowerEdge R630.

The hardware, hypervisors, and BIG-IP software are included in the TOE boundary.

The customer is responsible for acquiring and installing the hardware and hypervisor and ensuring that the hardware and hypervisor on which the TOE software will run are free of tampering. Refer to the manufacturers of those components for details.

The TOE software is delivered via download in the form of a virtual edition (VE) image fileset that is protected via a digital signature. The TOE guidance is delivered via download in the form of an ISO image along with a SHA-256 checksum for verification by the customer.

The ST claims exact conformance to Collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 24-September-2018.

The NIT technical decisions that have been applied to the Network Device Collaborative Protection Profile can be found in the ST.

There are seven assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the nine threats and comply with the one organisational security policy (OSP) in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB and was completed 2020-10-22. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 1 + ASE_SPD.1 and in accordance with the NDcPP Evaluation Activities.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2019022
Name and version of the certified IT product	BIG-IP LTM+APM Version 14.1.2 (build BIGIP-14.1.2-0.89.37, also referred to as 14.1.2 + EHF) with Appliance Mode licensed. Running on any of the following hypervisors: • VMWare ESXi 6.5.0 - Intel Xeon E5-2697v4 processor • Hyper-V version 10.0 on Windows Server 2019 - Intel Xeon E5-2660v3 processor • KVM on Centos 7 - Intel Xeon E5-2660v3 processor
Security Target Identification	F5 BIG-IP® 14.1.2 VE for LTM+APM Security Target, F5 Networks, Inc., 2020-03-31, Version 4.7
EAL	EAL 1 + ASE_SPD.1 and NDcPP V2.1
Sponsor	F5 Networks, Inc.
Developer	F5 Networks, Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.23.2
Scheme Notes Release	16.0
Recognition Scope	CCRA
Certification date	2020-11-04

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Function Management
- Protection of the TSF
- TOE Access
- Trusted Path / Channels

3.1 Security Audit

The TOE implements implements syslog capabilities to generate audit records for security relevant events. In addition, the TOE protects the audit trail from unauthorized modifications and loss of audit data due to insufficient space..

3.2 Cryptographic Support

The TOE provides cryptographic functionality is provided by the OpenSSL cryptographic module. The TOE provides a secure shell (SSH) to allow administrators to connect over a dedicated network interface. The TOE also implements the TLS protocol to allow administrators to remotely manage the TOE. The TOE implements a TLS client for interactions with other TLS servers. These cryptographic implementations utilize the cryptographic module which provides random number generation, key generation, key establishment, key storage, key destruction, hash operations, encryption/decryption operations, and digital signature operations.

3.3 User Data Protection

The TOE implements residual information protection on network packets traversing through it. In other words, network packets traversing through the BIG-IP do not contain any residual data.

3.4 Identification and Authentication

The TOE provides an internal password-based repository that is implemented for authentication of management users. The TOE enforces a strong password policy and disabling user accounts after a configured number of failed authentication attempts.

3.5 Security Function Management

A command line interface (available via the traffic management shell "tmsh"), web-based GUI ("Configuration utility"), a SOAP-based API ("iControl API"), and a REST-based API (“iControl REST API”) are offered to administrators for all relevant configuration of security functionality.

The TOE manages configuration objects in a partition which includes users, server pools, etc. This includes the authentication of administrators by user name and password, as well as access control based on pre-defined roles and, optionally, groups of objects ("Profiles"). "Profiles" can be defined for individual servers and classes of servers that the TOE forwards traffic from clients to, and for traffic that matches certain characteristics, determining the kind of treatment applicable to that traffic. Management capabilities offered by the TOE include the definition of templates for certain configuration options. The management functionality also implements roles for separation of duties.

3.6 Protection of the TSF

The TOE implements many capabilities to protect the integrity and management of its own security functionality. These capabilities include the protection of sensitive data, such as passwords and keys, self-tests, product update verification, and reliable time stamping.

3.7 TOE Access

Prior to interactive user authentication, the TOE can display an administrative defined banner. The TOE terminates interactive sessions after an administrator-defined period of inactivity and allows users to terminate their own authenticated session.

3.8 Trusted Path / Channels

The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers using TLS.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes seven assumptions on the usage and the operational environment of the TOE.

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

A.NO_THRU_TRAFFIC_PROTECTION

The standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP.

It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities..

A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside..

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords, etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

4.2 Organisational Security Policies

The Security Target contains one Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.3 Clarification of Scope

The Security Target contains nine threats, which have been considered during the evaluation.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the firewall by nefarious means such as masquerading as an Administrator to the firewall, masquerading as the firewall to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target firewalls that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or firewall credentials for use by the attacker.

T.PASSWORD_CRACKING

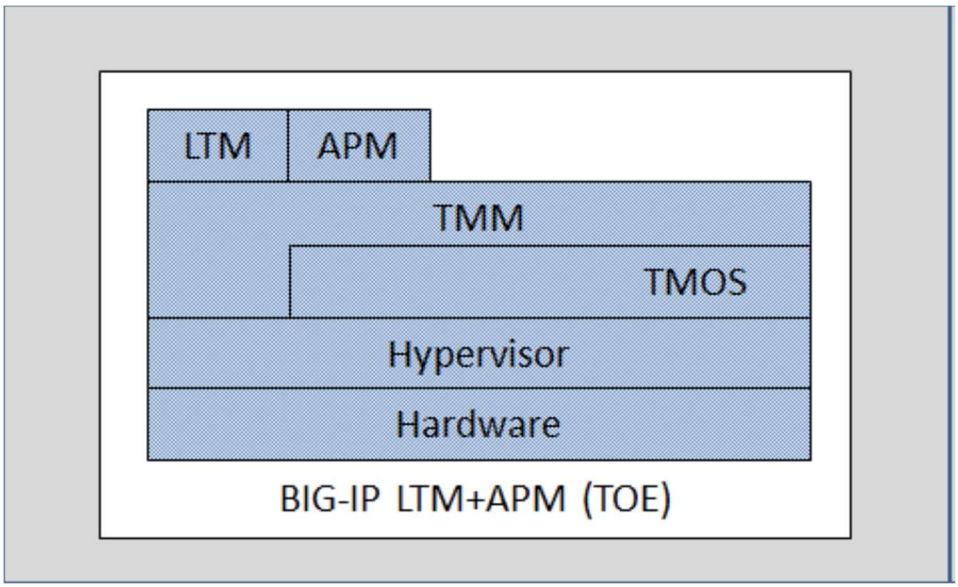
Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5 Architectural Information

The following diagram shows the basic components that comprise the TOE.



The TOE is separated into two (2) distinct planes, the control plane and the data plane. The control plane validates, stores, and passes configuration data to all necessary systems. It also provides all administrative access to the TOE. The data plane passes user traffic through the TOE.

The TOE implements and supports the following network protocols: TLS (client and server), SSH, HTTPS, FTP. The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers using TLS (TLSv1.1 and TLSv1.2). The cryptographic functionality implemented in the TOE is provided by OpenSSL.

The TOE is divided into six (6) subsystems: Hardware, Hypervisor, Traffic Management Operating System (TMOS), Traffic Management Micro-kernel (TMM), Local Traffic Manager (LTM), and Access Policy Manager (APM). F5's TMOS is a Linux-based operating system customized for performance. The TMM is the data plane of the product and all data plane traffic passes through the TMM. The LTM controls network traffic coming into or exiting the local area network (LAN) and provides the ability to intercept and redirect incoming network traffic. The APM module terminates TLS-based VPN connections from remote clients although these features are not included in the evaluated configuration.

At the core of BIG-IP is a concept referred to as Traffic Management Microkernel (TMM), representing the data plane of the product when compared to traditional network device architectures. It is implemented by a daemon running with root privileges, performing its own memory management, and having direct access to the hypervisor. TMM implements a number of sequential filters both for the "client-side" and "server-side" network interfaces served by BIG-IP. The filters implemented in TMM include a TCP, TLS, compression, and HTTP filter, amongst others. If the hypervisor provides more than one CPU, TMM runs multi-threaded (one thread per CPU). In this case, disaggregators in the kernel are responsible for de-multiplexing and multiplexing network traffic for handling by an individual TMM thread.

Additional plug-in filters can be added to this queue by individual product packages. These plug-ins typically have a filter component in TMM, with additional and more complex logic in a counter-part implemented in a Linux-based daemon (module). The plug-in modules relevant to this evaluation include:

- Local Traffic Manager (LTM): authentication of HTTP (based on Apache) traffic and advanced traffic forwarding directives
- Access Policy Manager (APM): TLS-based client connectivity.

6 Documentation

Relevant guidance documents for the secure operation of BIG-IP that are part of the TOE are:

- BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP LTM+AFM and BIG-IP LTM+APM Release 14.1.2 VE
- K05254775: Common Criteria Certification for BIG-IP 14.1.2 VE
- BIG-IP Device Service Clustering: Administration
- BIG-IP Digital Certificates: Administration
- BIG-IP Local Traffic Manager: Implementations
- BIG-IP Local Traffic Manager: Monitors Reference
- BIG-IP Local Traffic Manager: Profiles Reference
- BIG-IP Release Note
- BIG-IP System: Essentials
- BIG-IP System: SSL Administration
- BIG-IP System: User Account Administration
- BIG-IP Systems: Getting Started Guide
- BIG-IP TMOS: Implementations
- BIG-IP TMOS: Routing Administration
- External Monitoring of BIG-IP Systems: Implementations
- GUI Help Files
- iControl SDK
- iControl REST API User Guide
- K12042624: Restricting access to the Configuration utility using client certificates (12.x – 14.x)
- K13092: Overview of securing access to the BIG-IP system
- K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 14.x)
- K13454: Configuring SSH public key authentication on BIP-IP systems (11.x – 14.x)
- K14620: Managing SSL Certificates for BIG-IP systems using the Configuration utility
- K14783: Overview of the Client SSL profile (11.x – 14.x)
- K14806: Overview of the Server SSL profile (11.x – 15.x)
- K15497: Configuring a secure password policy for the BIG-IP system (11.x – 14.x)
- K15664: Overview of BIG-IP device certificates (11.x – 14.x)
- K42531434: Replacing the Configuration utility’s self-signed SSL certificate with a CA-signed SSL certificate
- K5532: Configuring the level of information logged for TMM-specific events
- K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system
- K7752: Licensing the BIG-IP system

- K80425458: Modifying the list of ciphers and MAC algorithms used by the SSH service on the BIGIP system or BIG-IQ system
- K9908: Configuring an automatic logout for idle sessions
- Traffic Management Shell (tmsh) Reference Guide (versions 14.1.0 and 12.0.01)
- BIG-IP VE in Linux KVM
- BIG-IP VE in Microsoft Hyper-V
- BIG-IP VE in VMware ESXi
- BIG-IP Virtual Edition Supported Platforms
- K14810: Overview of BIG-IP VE license and throughput limits
- K14946: Overview of BIG-IP VE image sizes
- Linux KVM – BIG-IP VE Setup
- Linux KVM – BIG-IP VE Users Guide
- Linux KVM – Configure cryptographic offload for BIG-IP VE with Intel QAT
- Microsoft Hyper-V – BIG-IP VE Setup
- Microsoft Hyper-V – BIG-IP VE Users Guide
- VMware ESXi – BIG-IP VE Setup
- VMware ESXi – BIG-IP VE Users Guide

7 IT Product Testing

7.1 Evaluator Testing

The independent testing was performed on the TOE in the form that it is delivered to customers. The evaluator has performed more than 50 test cases, including extensive testing to test cryptographic protocols (SSH, TLS, HTTPS) as well as underlying cryptographic operations (FCS_COP, FCS_CKM) that were also separately tested in algorithm testing. All test cases passed successfully.

Algorithm testing is required to be performed by the NDcPP Supporting Document [EA-ND 2.1]. Algorithm test vectors were generated by CAVS tool to test all cryptographic algorithms of the TOE. The testing is valid for all hypervisors supported by the TOE, which is evident from the certificates: KVM, VMware and Hyper-V.

7.2 Penetration Testing

The approach for the penetration test was to scan all TCP/IP ports on the TOE platform to identify all open ports. The penetration test was performed on the TOE in the evaluated configuration. The results of the port scan found that there were no open ports.

8 Evaluated Configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- Appliance mode is licensed. This results in root access to the TOE operating system and bash shell being disabled.
- Certificate validation is performed using CRLs.
- Disabled interfaces:
  - All command shells other than tmsh are disabled. For example, bash and other user-serviceable shells are excluded.
  - Management of the TOE via SNMP is disabled.
  - Management of the TOE via the appliance's LCD display is disabled.
  - SSH client

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Functional Specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.1	PASS
CM Scope	ALC_CMS.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing	ATE_IND.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS
Evaluation Activities for NDcPP		PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CRL	Certificate Revocation List
EAL2	Evaluation Assurance Level 2
GUI	Graphical User Interface
ITSEF	IT Security Evaluation Facility
LTM	Local Traffic Manager
OSP	Organisational Security Policy
PP	Protection Profile
SOAP	Simple Object Access Protocol
ST	Security Target
TLS	Transport Layer Security
TMM	Traffic Management Microkernel
TMOS	Traffic Management Operating System
TOE	Target of Evaluation
TSF	TOE Security Functions
vCMP	Virtual Clustered Multi-Processing
VE	Virtual Edition

12 Bibliography

ST	F5 BIG-IP 14.1.0 for LTM+AFM Security Target, F5 Networks Inc. 2019-07-10 document version 4.6
ECG	BIG-IP Common Criteria Evaluation Configuration Guide BIG-IP LTM+AFM and BIG-IP LTM+APM Release 14.1.2 VE, F5 Networks Inc., 2020-10-16, document version 4.75
NDcPP	Collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 2018-09-24, document version 2.1
EA-ND 2.1	Evaluation Activities for Network Device cPP, september-2018, document version 2.1
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-09-24, document version 31.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.23.2". The certifier concluded that, from QMS 1.23 to the current QMS 1.23.2, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test Coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 21 - NIAP PP Certifications
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 23 - Evaluation reports for NIAP PPs and cPPs
- Scheme Note 25 - Use of CAVP-tests in CC evaluations