Swedish Certification Body for IT Security

Certification Report F5 BIG-IP v17.1.0.1 APM

Issue: 1.0, 2024-okt-11

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a networking device comprised of hardware and software. The TOE provides network traffic management functionality, e.g. local traffic management and access policy management. TOE consists of the software version 17.1.0.1 including APM, build 17.1.0.1- 0.61.4, installed on one of the following hardware appliances:

- i4000 model series, including i4600, and i4800
- i5000 model series, including i5600, i5800, and i5820-DF
- i7000 model series, including i7600, i7800, and i7820-DF
- i10000 model series, including i10600, and i10800
- i11000-DS model series, including i11600-DS, and i11800-DS
- i15000 model series, including i15600, i15800 and i15820-DF
- C2400 with B2250
- C4480 with B4450
- R4000 model series, including R4600 and R4800
- R5000 model series, including R5600, R5800, R5900, and R5920-DF
- R10000 model series, including R10600, R10800, R10900, and R10920-DF
- R12000 model series, including R12600DS, R12800DS, and R12900DS
- CX410 with BX110

TOE is also available for the following hypervisors

- VMWare ESXi 8.0.0.10100
- Hyper-V 10.0.20348.1 on Windows Server 2022 Standard
- KVM qemu-system-x86 v1:6.2+dfsg-2ubuntu6.6 on Ubuntu 22.04.1 LTS

The TOE hardware appliances above are delivered via common carrier from an authorized subcontractor. The TOE software is downloaded from the F5 website.

The Security Target [ST] claims exact conformance to the Collaborative Protection Profile for Network Devices version 2.2e [NDcPP].

A list of the NIT technical decisions considered during the evaluation is available in the ST.

There are eleven assumptions being made in the ST regarding the secure usage and the operational 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, threats, 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 in 2024-Sep-23. 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. The evaluation meets the requirements of evaluation assurance level EAL 1, augmented by ASE_SPD.1 Security Problem Definition and the NDcPP Evaluation Activities [SD NDcPP].

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 Evaluation Activities for Collaborative Protection Profile for Network Devices [SD NDcPP].

The technical information in this report is based on the Security Target and the Final Evaluation Report (FER) produced by atsec information security AB.

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	CSEC2023002
Name and version of the certified IT product	F5 BIG-IP v17.1.0.1 including APM build 17.1.0.1-0.61.4
Security Target Identification	F5 BIG-IP 17.1.0.1 including APM Security Target, F5 Inc., 2024-September-09, document version 7.11
EAL	EAL 1 + ASE_SPD.1 (NDcPP v2.2e)
Sponsor	F5 Inc.
Developer	F5 Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.5.2
Scheme Notes Release	22.0
Recognition Scope	CCRA, EA/MLA
Certification date	2024-Oct-11

3 Security Policy

The TOE provides the following security services:

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

3.1 3.1 Security Audit

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

3.2 3.2 Cryptographic Support

In BIG-IP, cryptographic functionality is provided by the OpenSSL cryptographic module. The BIG-IP provides a secure shell (SSH) to allow administrators to connect over a dedicated network interface. BIG-IP also implements the TLS protocol to allow administrators to remotely manage the TOE. BIG-IP 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 3.3 Identification and Authentication

An internal password-based repository is implemented for authentication of management users. BIG-IP enforces a strong password policy and disabling user accounts after a configured number of failed authentication attempts.

3.4 3.4 Security Management

A command line interface (available via the traffic management shell "tmsh"), web-based GUI ("Configuration utility" or “TMUI”), 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.

3.5 3.5 Protection of the TSF

BIG-IP 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.

3.6 3.6 TOE Access

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

3.7 3.7 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 on Usage and Environment

The Security Target [ST] makes eleven 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. For vNDs, this assumption applies to the physical platform on which the VM runs.

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).
In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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.

A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)
The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

A.VS_REGULAR_UPDATES (applies to vNDs only)
The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.VS_ISOLATON (applies to vNDs only)
For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

A.VS_CORRECT_CONFIGURATION (applies to vNDs only)
For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs

4.2 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 Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device 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 Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device 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 Network Devices that do not use standardized secure tunnelling 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 Network Device 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 Network Device 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 Network Device 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 device data enabling continued access to the Network Device 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 device 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 device. Having privileged access to the device 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.

The Security Target contains one Organisational Security Policy (OSP), 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.

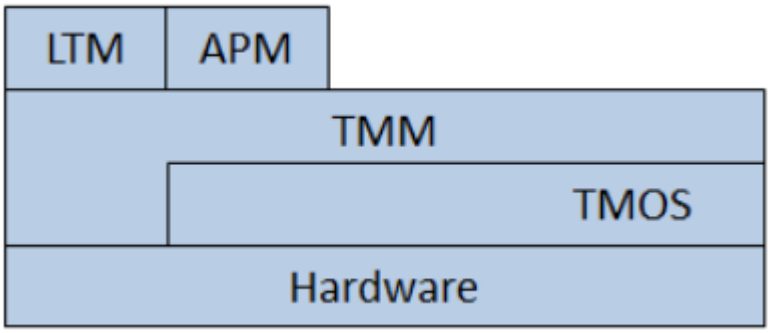
5 Architectural Information

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.

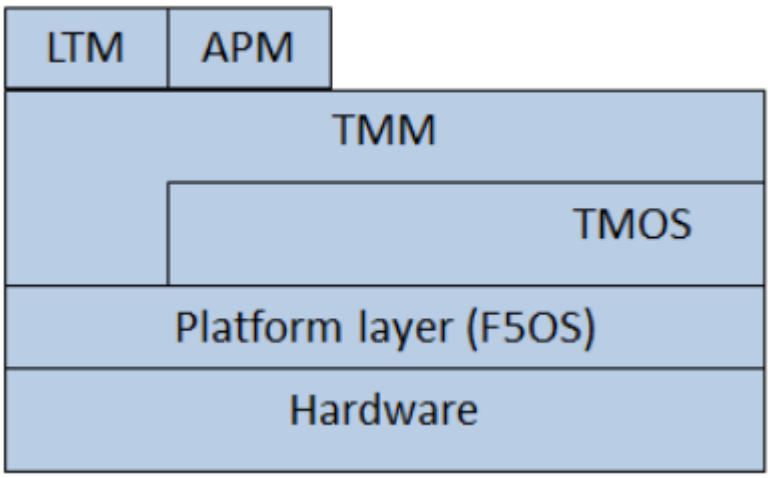
The TOE implements and supports the following network protocols: TLS (client and server), SSH, HTTPS, FTP. The TOE protects remote connections to its management interfaces with TLS and SSH. The TOE also protects communication channels with audit servers using TLS (TLSv1.1 and TLSv1.2). The cryptographic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

The TOE is divided into the following subsystems:

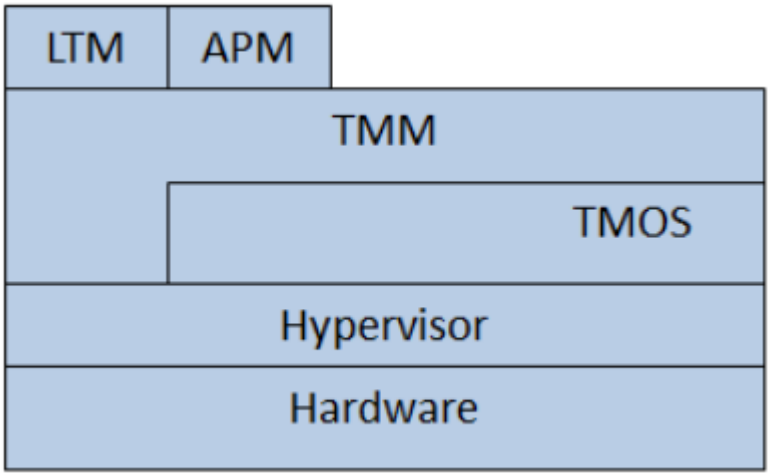
- F5 Device Hardware,
- F5 platform layer for rSeries and VELOS devices,
- Hardware for hypervisor deployments,
- Hypervisor for hypervisor deployments,
- Traffic Management Operating System (TMOS),
- Traffic Management Micro-kernel (TMM),
- Access Policy Manager (APM), and
- Local Traffic Manager (LTM).



BIG-IP Subsystems for F5 devices (except rSeries and VELOS)



BIG-IP subsystems for F5 rSeries and VELOS devices



BIG-IP subsystems for virtual deployments with hypervisors

6 Documentation

The main guide to installing the TOE into the evaluated configuration is:

[ECG] BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP® Release 17.1.0.1

The [ST], section 1.6.3.2 provides a full list of the guidance documents that are part of the TOE.

The TOE documentation is collected in an ISO file that can be downloaded via https from the F5 website.

7 IT Product Testing

7.1 Evaluator Testing

The cryptographic testing was performed within the Cryptographic Algorithm Validation Program (CAVP). The CAVP certificates covers all TOE hardware appliances, and the following third party hypervisor configurations:

- VMWare ESXi 8.0.0 on Intel Xeon Gold 6330N processor
- Hyper-V 10.0 on Windows Server 2022 and Intel Xeon Silver 4309Y processor
- KVM on Ubuntu 22.04.1 LTS and Intel Xeon Silver 4309 processor

All other tests were performed on the i7800, r5900, and the r12900 models, on the VELOS CX410 with BX410, and a virtual deployment on VMWare ESXi 8.0.0, all with the software build 17.1.0.1-0.61.4.

The evaluator testing was successful and did not reveal any errors.

7.2 Penetration Testing

Portscanning was performed to find open ports that should not be open on the i7800, r5900, and the r12900 models, on the VELOS CX410 with BX410, and a virtual deployment on VMWare ESXi 8.0.0, all with the software build 17.1.0.1-0.61.4.

No discrepancies were found during the penetration testing

8 Evaluated Configuration

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

- Appliance mode is licensed. Appliance mode disables root access to the TOE operating system and disables bash shell.
- 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. (applicable to F5 devices)
  - Remote (i.e., SSH) access to the Lights Out / Always On Management capabilities of the system is disabled. (applicable to F5 devices)
  - 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 evaluators also applied all assurance activities implied by the collaborative PP [NDcPP].

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC] and the evaluation activities implied by the collaborative PP [NDcPP].

The evaluators' overall verdict is PASS.

The verdicts for the respective 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

ADC	Application Delivery Controller
AFM	Advanced Firewall Manager
APM	Access Policy Manager
CA	Certificate Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CRL	Certificate Revocation List
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LTM	Local Traffic Manager
NDcPP	Network Device Collaborative Protection Profile
OS	Operating System
PP	Protection Profile
SHA	Secure HashAlgorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TMM	Traffic Management Microkernel
TMOS	Traffic Management Operating System
tmsh	Traffic management shell
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol

12 Bibliography

ST	F5 BIG-IP® 17.1.0.1 including APM Security Target, F5 Inc., 2024-September-09, document version 7.11
ECG	BIG-IP® Common Criteria Evaluation Configuration Guide BIG-IP Release 17.1.0.1, F5 Inc., 03/08/2024, document version 7.7
NDcPP	collaborative Protection Profile for Network Devices, 2020-03-23, document version 2.2e
SD NDcPP	Supporting Document - Evaluation Activities for Network Device cPP, 2019-12-20, document version 2.2
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

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

Version	Introduced	Impact of changes
2.5.2	2024-06-14	None.
2.5.1	2024-02-29	None.
2.5	2024-01-25	None.
2.4.1	2023-09-14	None.
2.4	2023-06-15	None.
2.3.1	2023-04-20	None.
2.3	Application	Original version

A.2 Scheme Notes

Scheme Note 18 - ST Requirements
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
Scheme Note 27 - ST requirements at the time of application for certification
Scheme Note 28 - Updated procedures for application, evaluation ad certification