National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Application Software

Version 1.4

07 October 2021

Report Number: CCEVS-VR-PP-0080
Dated: 23 January 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
UL Verification Services Inc. (Formerly InfoGard)
San Luis Obispo, CA 93401

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Application Software, Version 1.4 (PP_APP_V1.4). It presents a summary of the PP_APP_V1.4 and the evaluation results.

UL Verification Services Inc. (Formerly InfoGard), located in San Luis Obispo, CA, performed the evaluation of PP_APP_V1.4 concurrent with the first product evaluation against the PP's requirements. The evaluated product was Bastille Enterprise Fusion Center Version 3.2.0.

This evaluation addressed the base security functional requirements of PP_APP_V1.4. This evaluation also addressed several of the additional requirements contained in the appendices of PP_APP_V1.4.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that PP_APP_V1.4 is both Common Criteria Part 2 extended and Part 3 extended. The PP identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from the PP_APP_V1.4; completion of the ASE workunits satisfied the APE workunits for PP_APP_V1.4, but only for those parts of the ST that were relevant to this PP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs that contain Evaluation Activities, which are interpretations of CEM workunits specific to the technology described by the PP.

To promote thoroughness and efficiency, the evaluation of PP_APP_V1.4 was performed concurrent with the first product evaluation against the PP's requirements. In this case, the Target of Evaluation (TOE) was Bastille Enterprise Fusion Center, evaluated by UL Verification Services Inc. (Formerly InfoGard) in San Luis Obispo, CA, United States of America.

This evaluation addressed the base security functional requirements of PP_APP_V1.4. This PP also defines additional requirements, some of which the Bastille product evaluation claimed.

PP_APP_V1.4 contains a set of base requirements that all conformant STs must include, and additionally contains optional, selection-based, and objective requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against PP_APP_V1.4. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include references to this as additional evidence that the corresponding portions of PP_APP_V1.4 were evaluated.

The following identifies the PP subject of the evaluation or validation, as well as the supporting information from the evaluation performed against this PP.

Protection Profile	Protection Profile for Application Software, Version 1.4, 07 October 2021
ST (Base)	Bastille Enterprise Fusion Center Version 3.2.0 Security Target, Version 0.9.3, 03 September 2022
Assurance Activity Report (Base)	Assurance Activity Report Bastille Networks, Inc. Bastille Enterprise Fusion Center Version 3.2.0, Version 1.3, 02 September 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	UL Verification Services Inc. (Formerly InfoGard) San Luis Obispo, CA

3 PP_APP_V1.4 Description

The PP_APP_V1.4 specifies information security requirements for application software, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

The application, which consists of the software provided by its vendor, is installed onto the platform(s) it operates on. It executes on the platform, which may be an operating system, hardware environment, a software based execution environment, or some combination of these. Those platforms may themselves run within other environments, such as virtual machines or operating systems, that completely abstract away the underlying hardware from the application. The TOE is not accountable for security functionality that is implemented by platform layers that are abstracted away.

Applications include a diverse range of software such as office suites, thin clients, PDF readers, downloadable smartphone apps, and apps running in a cloud container. The TOE includes any software in the application installation package, even those pieces that may extend or modify the functionality of the underlying platform, such as kernel drivers.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

4.2 Threats

The following table contains applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter

Threat Name	Threat Definition
	communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

4.3 Organizational Security Policies

This protection profile contains no organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this

TOE Security Objective	TOE Security Objective Definition
	data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

The following table contains security objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5 Requirements

As indicated above, requirements in the PP_APP_V1.4 are comprised of the "base" requirements and additional requirements that are optional, selection-based, or objective. The following table contains the "base" requirements that were validated as part of the UL Verification Services Inc. (Formerly InfoGard) evaluation activities referenced above.

Table 5: Base Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation Services	Bastille Enterprise Fusion Center Version 3.2.0
	FCS_RBG_EXT.1: Random Bit Generation Services	Bastille Enterprise Fusion Center Version 3.2.0
	FCS_STO_EXT.1: Storage of Credentials	Bastille Enterprise Fusion Center Version 3.2.0
FDP: User Data Protection	FDP_DAR_EXT.1: Encryption of Sensitive Application Data	Bastille Enterprise Fusion Center Version 3.2.0
	FDP_DEC_EXT.1: Access to Platform Resources	Bastille Enterprise Fusion Center Version 3.2.0
	FDP_NET_EXT.1: Network Communications	Bastille Enterprise Fusion Center Version 3.2.0
FMT: Security Management	FMT_CFG_EXT.1: Secure by Default Configuration	Bastille Enterprise Fusion Center Version 3.2.0
	FMT_MEC_EXT.1: Supported Configuration Mechanism	Bastille Enterprise Fusion Center Version 3.2.0
	FMT_SMF.1: Specification of Management Functions	Bastille Enterprise Fusion Center Version 3.2.0
FPR: Privacy	FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information	Bastille Enterprise Fusion Center Version 3.2.0
FPT: Protection of the TSF	FPT_AEX_EXT.1: Anti-Exploitation Capabilities	Bastille Enterprise Fusion Center Version 3.2.0
	FPT_API_EXT.1: Use of Supported Services and APIs	Bastille Enterprise Fusion Center Version 3.2.0
	FPT_IDV_EXT.1: Software Identification and Versions	Bastille Enterprise Fusion Center Version 3.2.0
	FPT_LIB_EXT.1: Use of Third Party Libraries	Bastille Enterprise Fusion Center Version 3.2.0
	FPT_TUD_EXT.1: Integrity for Installation and Update	Bastille Enterprise Fusion Center Version 3.2.0
FTP: Trusted Path/Channel	FTP_DIT_EXT.1: Protection of Data in Transit	Bastille Enterprise Fusion Center Version 3.2.0

The following table contains the "**Strictly Optional**" requirements contained in Appendix A.1, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE workunits and has indicated its verification through "PP Evaluation."

Table 6: Optional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1/SK: Cryptographic Symmetric Key Generation	PP Evaluation

The following table contains the "**Objective**" requirements contained in Appendix A.2, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE workunits and has indicated its verification through "PP Evaluation."

Table 7: Objective Requirements

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_API_EXT.2: Use of Supported Services and APIs	PP Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE workunits and has indicated its verification through "PP Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1/AK: Cryptographic Asymmetric Key Generation	PP Evaluation
	FCS_CKM.1/PBKDF: Password Conditioning	PP Evaluation
	FCS_CKM.2: Cryptographic Key Establishment	PP Evaluation
	FCS_COP.1/SKC: Cryptographic Operation – Encryption/Decryption	PP Evaluation
	FCS_COP.1/Hash: Cryptographic Operation - Hashing	PP Evaluation
	FCS_COP.1/Sig: Cryptographic Operation - Signing	PP Evaluation
	FCS_COP.1/KeyedHash: Cryptographic Operation – Keyed-Hash Message Authentication	PP Evaluation
	FCS_HTTPS_EXT.1/Client: HTTPS Protocol	PP Evaluation
	FCS_HTTPS_EXT.1/Server: HTTPS Protocol	PP Evaluation
	FCS_HTTPS_EXT.2: HTTPS Protocol with Mutual Authentication	PP Evaluation
	FCS_RBG_EXT.2: Random Bit Generation from Application	PP Evaluation

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_X509_EXT.1: X.509 Certificate Validation	Bastille Enterprise Fusion Center Version 3.2.0
	FIA_X509_EXT.2: X.509 Certificate Authentication	Bastille Enterprise Fusion Center Version 3.2.0
FPT: Protection of the TSF	FPT_TUD_EXT.2: Integrity for Installation and Update	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the PP_APP_V1.4.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ADV: Development	ADV_FSP.1 Basic Functional Specification	Bastille Enterprise Fusion Center Version 3.2.0
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Bastille Enterprise Fusion Center Version 3.2.0
	AGD_PRE.1: Preparative Procedures	Bastille Enterprise Fusion Center Version 3.2.0
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Bastille Enterprise Fusion Center Version 3.2.0
	ALC_CMS.1: TOE CM Coverage	Bastille Enterprise Fusion Center Version 3.2.0
	ALC_TSU_EXT.1: Timely Security Updates	Bastille Enterprise Fusion Center Version 3.2.0
ATE: Tests	ATE_IND.1: Independent Testing – Conformance	Bastille Enterprise Fusion Center Version 3.2.0
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Bastille Enterprise Fusion Center Version 3.2.0

7 Results of the Evaluation

Note that for APE elements and workunits that are identical to ASE elements and workunits, the lab performed the APE workunits concurrent to the ASE workunits.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Bastille Enterprise Fusion Center Version 3.2.0
APE_ECD.1	Pass	Bastille Enterprise Fusion Center Version 3.2.0
APE_INT.1	Pass	Bastille Enterprise Fusion Center Version 3.2.0

APE Requirement	Evaluation Verdict	Verified By
APE_OBJ.2	Pass	Bastille Enterprise Fusion Center Version 3.2.0
APE_REQ.2	Pass	Bastille Enterprise Fusion Center Version 3.2.0
APE_SPD.1	Pass	Bastille Enterprise Fusion Center Version 3.2.0

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the PP_APP_V1.4 Evaluation Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[7] Bastille Enterprise Fusion Center Version 3.2.0 Security Target, Version 0.9.3, 03 September 2022

[8] Assurance Activity Report Bastille Networks, Inc. Bastille Enterprise Fusion Center Version 3.2.0, Version 1.3, 03 September 2022