National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

HCL BigFix Server Version 11.0.3

Report Number: CCEVS-VR-VID11481-2025
Dated: May 27. 2025
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

Validation Team

Lisa Mitchell

Lori Sarem

Chris Thorpe

The MITRE Corporation

Russ Fink

John Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Joachim Vandersmissen

Hunter Barton

atsec information security corporation

Austin, TX

Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of HCL BigFix Server Version 11.0.3. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End- users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by atsec Common Criteria Testing Laboratory (CCTL) in Austin, TX, USA, and was completed in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by atsec. The evaluation determined that the TOE is Common Criteria Part 2 Extended and Common Criteria Part 3 Extended and meets the assurance requirements of the *Protection Profile for Application Software*, Version 1.4, 2021-10-07 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 2019-03-01.

The Target of Evaluation (TOE) is the HCL BigFix Server Version 11.0.3.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *HCL BigFix Server Version 11.0.3 Security Target*, Version 1.2, 2025-05-06 and analysis performed by the validation team.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	HCL BigFix Server Version 11.0.3
PP	*Protection Profile for Application Software*, Version 1.4, 2021-10-07 *Functional Package for Transport Layer Security (TLS),* Version 1.1, 2019-03-01
Security Target	*HCL BigFix Server Version 11.0.3 Security Target,* Version 1.2, 2025-05-06
Evaluation Technical Report	*Evaluation Technical Report for HCL BigFix Server Version 11.0.3*, Version 1.3, 2025-05-23
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	HCL Technologies Limited
CCTL	atsec information security corporation 4516 Seton Center Parkway Suite 250 Austin, TX 78759
Evaluation Personnel	Joachim Vandersmissen, Hunter Barton
Validation Personnel	Lisa Mitchell, Lori Sarem, Chris Thorpe, Russ Fink

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST.

The TOE is part of the HCL BigFix Endpoint Management solution (a.k.a. HCL BigFix platform), a centralized endpoint management system that allows authorized operators to monitor the system configurations of distributed endpoint systems (client computers) and enables operators to take any necessary corrective actions.

HCL BigFix Endpoint Management utilizes a patented Fixlet® technology to identify vulnerable or misconfigured computers in the enterprise and allows authorized users to remediate identified issues across the network.

The Fixlet messages are available to an enterprise by subscribing to any of several Fixlet Sites that are maintained by HCL. Each Fixlet Site contains pre-tested, pre-packaged Fixlet messages that provide out-of-the-box management solutions. They constitute data that the BigFix system collects, distributes, and utilizes to detect and remediate vulnerabilities.

3.1 TOE Description

The BigFix server is the TOE and implements the server functionality of HCL BigFix Endpoint Management solution. The TOE runs as a Windows service and provides the following features:

- Maintain a database of enrolled endpoints and subscribed software.
- Accept the enrollment of new endpoints.
- Search and gather software updates and/or endpoint configuration updates (known as Fixlets) for subscribed software from multiple Internet-based HCL Fixlet Sites.
- Download necessary software patches from the vendor sites.
- Provide management services to the Console and REST API applications to administrate endpoints, Fixlets, and corrective actions.
- Distribute Fixlets and corrective actions to enrolled endpoints.
- Receive reports and status updates from enrolled endpoints.

The TOE implements secure channels using the HTTPS protocol to protect all the information flowing between the TOE and other trusted IT products. The TOE does not implement mutual authentication.

The TOE includes the OpenSSL cryptographic module to implement the TLS protocol. The TOE implements the HTTPS Client using the cURL library which uses OpenSSL and is part of the TOE. The TOE implements the HTTPS Server using OpenSSL for TLS and the Windows Sockets (Winsock) API for lower-level sockets. Winsock is provided by the underlying platform; the OpenSSL API is provided by the OpenSSL cryptographic module part of the TOE.

The TOE supports the TLS protocol versions 1.2 and 1.3 for HTTPS implementation. This ST claims conformance to Functional Package for Transport Layer Security (TLS) Version 1.1 [PKG_TLS_V1.1], which does not cover TLS version 1.3. Therefore, TLS version 1.3 is out of scope of this evaluation and this ST focuses on TLS version 1.2.

The TOE claims compliance to the Application Software Protection Profile Version 1.4 [PP_APP_V1.4].

The TOE falls under use case 3 ("Communication") described in section 1.4 of the PP.

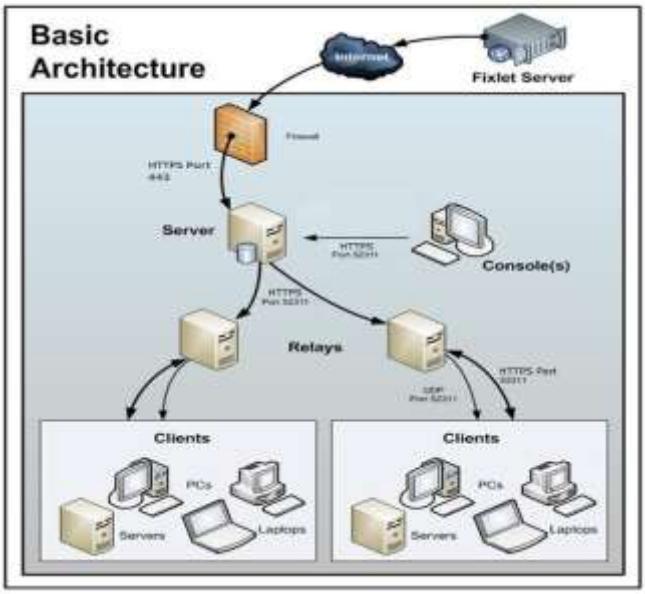
3.2 TOE Evaluated Platform

Details regarding the evaluated configuration are provided in Section 8.

3.3 TOE Architecture

The BigFix platform is comprised of the following main components as shown in the figure below:

- BigFix Server (a.k.a. Server), the TOE.
- BigFix Administration Tool (a.k.a. Admin Tool).
- BigFix Console (a.k.a. Console).
- BigFix IEM Command-Line Interface (a.k.a. IEM CLI).
- BigFix Client (a.k.a. Client or Agent).
- BigFix Relay (a.k.a. Relay).



3.4 Physical Boundaries

The physical boundary of the TOE consists of the application installer executable and guidance documentation.

The TOE installer is bundled in the BigFix platform installation package that can be obtained from the BigFix Enterprise Suite Download Center. The TOE also includes the TOE guidance listed below, which provides information for installing, configuring, and maintaining the evaluated configuration:

- *HCL BigFix Server Version 11.0.3 Common Criteria Configuration Guide* [CCGUIDE]

The hardware platform used during the evaluation was a Dell PowerEdge R430 with Intel Broadwell Xeon E5-2620 v4 processor.

For the evaluated configuration, the TOE requires the following software components installed in the same machine:

- Microsoft Windows Server 2019 Standard version 1809
- Microsoft SQL Server 2019

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channel

4.1 Cryptographic Support

The TOE provides cryptographic support using the OpenSSL cryptographic module that is bundled in the TOE, and Windows Cryptography API: Next Generation (CNG), which is provided by the underlying Windows platform.

The TOE uses the OpenSSL cryptographic module for the following security functionality:

- Trusted channels for incoming and outgoing connections using the TLS protocol version 1.2.
- Conditioning of passwords for storing credentials (Master Operator's and Operator's passwords).

The TOE uses the Windows CNG for the following cryptographic services:

- Protect private keys and database credentials using the Data Protection Application Programming Interface (DPAPI).
- Provide entropy to the SP800-90A compliant DRBG implemented in the OpenSSL cryptographic module.

4.2 User Data Protection

The TOE provides user data protection by encrypting sensitive data at rest, as well as restricting access to platform-based resources required by the TOE.

4.3 Identification and Authentication

The TOE authenticates the identity of the endpoint server when connecting as a TLS client by validating the X.509 certificates received from the server during the TLS protocol handshake. The TOE uses the cURL library and the OpenSSL cryptographic module, which are part of the TOE.

4.4 Security Management

The TOE provides cryptographic support using the OpenSSL cryptographic module that is bundled in the TOE, and Windows Cryptography API: Next Generation (CNG), which is provided by the underlying Windows platform.

4.5 Privacy

The TOE does not request Personally Identifiable Information (PII).

4.6 Protection of the TSF

The TOE implements several mechanisms to protect itself and its security functionality. These mechanisms include utilizing only documented Windows platform APIs; not writing user-modifiable files to directories that contain its executable files; using stack buffer overrun protection and Address Space Layout Randomization (ASLR) techniques.

All TOE binaries and updates are signed using the Microsoft Authenticode process. The TOE is delivered as an InstallShield installation package, signed by HCL America Inc.

4.7 Trusted Path/Channel

The TOE protects all incoming and outgoing transmitted data by using trusted channels with HTTPS, using the TLS version 1.2 as the underlying protocol. The TOE implements the TLS protocol using the OpenSSL cryptographic module which is part of the TOE.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- 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 for the TOE.
- 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.
- The user of the application software is not willfully negligent or hostile and uses the software in compliance with the applied enterprise security policy.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the PP_APP_v1.4/PKG_TLS_V1.1 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance, achieved through performance by the evaluation team of the evaluation activities specified by the PP and functional package specified in *Table 1*.
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Security Target ([ST]) identified in *Table 1*. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor provides guidance documents describing the installation process for HCL BigFix Server Version 11.0.3, as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation is as follows:

- *HCL BigFix Server Version 11.0.3 Common Criteria Configuration Guide [CCGUIDE]*

Any additional documentation not mentioned above that may be provided on the vendor's website, was not covered by the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the evaluation team.

A non-proprietary description of the tests performed and their results is provided in the following document:

- *HCL BigFix Server Version 11.0.3 Assurance Activity Report*, Version 1.1, 2025-05-07 ([AAR]).

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the *PP* and *Functional Package* identified in *Table 1*.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team established a test configuration comprising the TOE running on a Dell PowerEdge R430 with Intel Broadwell Xeon E5-2620 v4 processor. The Assurance Activities Report ([AAR]) provides a detailed description of the test configuration the CCTL used to test the TOE.

The evaluation team devised a Test Plan based on the Test Activities specified in the *PP* and *Functional Package* identified in *Table 1*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the atsec CCTL facility in Austin, TX, from December 2024 to March 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE comprises HCL BigFix Server Version 11.0.3, installed on a Dell PowerEdge R430 with Intel Broadwell Xeon E5-2620 v4 processor.

8.2 Excluded Functionality

HCL BigFix Server additionally includes the following features that are not part of the evaluated TOE because they are outside the scope of the functionality described by the TOE's conformance claims:

The following BigFix components and features are not allowed in the evaluated configuration:

- BigFix Relay
- BigFix Web Reports
- BigFix WebUI
- BigFix Explorer
- BigFix Asset Discovery
- Disaster Server Architecture (DSA)

Additionally, the following constraints apply:

- The TOE must be configured to use "FIPS mode".
- The MSSQL database must reside in the same system as the TOE.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary *Evaluation Technical Report HCL BigFix Server Version 11.0.3* ([ETR]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([CCPART1], [CCPART2], [CCPART3]) and CEM version 3.1, revision 5 ([CEM]), and the specific evaluation activities specified in the *PP* and *Functional Package* identified in *Table 1*.

The evaluation team determined the TOE satisfies the conformance claims made in the Security Target [ST], of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in the *PP* and *Functional Package* specified in *Table 1*.

The validation team reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS evaluation activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed PPs, and security function descriptions that satisfy the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development Activities (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed PP for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Activities (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit to the extent possible given the evaluation evidence required by the claimed PP. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activities (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and Functional Package and recorded the results in the Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. The vulnerability analysis is in the Evaluation Test Report (ETR) prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team searched using the following sources:

- MITRE Common Vulnerabilities and Exposures (CVE) List:
  - https://cve.mitre.org/cve/search_cve_list.html
- National Vulnerability Database:
  - https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities Catalog:
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- OpenSSL Vulnerabilities:
  - https://openssl-library.org/news/vulnerabilities-3.0/
  - https://openssl-library.org/news/vulnerabilities-3.2/

The searches were performed during the evaluation, with the last search performed on 2025-05-05, using the following keywords:

- BigFix
- cURL
- libcurl
- ICU
- OpenSSL
- SQLite
- Xerces-C
- Zlib
- boost
- rapidxml
- Cryptography Next Generation

In addition to the lists of fixes published by the vendor, the evaluator performed manual searches throughout the evaluation process. The results of these searches did not identify any vulnerabilities.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the evaluation activities specified in the claimed PP. Furthermore, the evaluation team's testing demonstrates the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *HCL BigFix Server Version 11.0.3 Common Criteria Configuration Guide* [CCGUIDE]. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in PP_APP_V1.4/PKG_TLS_V1.1. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The ST for this product's evaluation is *HCL BigFix Server Version 11.0.3 Security Target*, Version 1.2, 2025-05-06 ([ST]).

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

CAVP Cryptographic Algorithm Validation Program

CC Common Criteria for Information Technology Security Evaluation

CCTL Common Criteria Testing Laboratory

CEM Common Evaluation Methodology

ETR Evaluation Technical Report

HTTPS Hypertext Transfer Protocol Secure

IT Information Technology

NIAP National Information Assurance Partnership

NIST National Institute of Standards and Technology

PCL Product Compliant List

PP Protection Profile

SAR Security Assurance Requirement

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functions

TSS TOE Summary Specification

VR Validation Report

14 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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature**. Part of a product that is either included with the product or can be ordered separately.
- **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.

15 Bibliography

The validation team used the following documents to produce this VR:

[CCPART1] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model*, Version 3.1, Revision 5, April 2017.

[CCPART2] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[CCPART3] *Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements*, Version 3.1, Revision 5, April 2017.

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

[PP_APP_V1.4] *Protection Profile for Application Software*, Version 1.4, 14 June 2021.

[PKG_TLS_V1.1] *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019.

[ST] *HCL BigFix Server Version 11.0.3 Security Target*, Version 1.2, 2025-05-06.

[CCGUIDE] *HCL BigFix Server Version 11.0.3 Common Criteria Configuration Guide*, Version 1.0, 2025-02-07.

[ETR] *Evaluation Technical Report HCL BigFix Server Version 11.0.3*, Version 1.3, 2025-05-23

[AAR] *HCL BigFix Server Version 11.0.3 Assurance Activity Report*, Version 1.1, 2025-05-07

[DTR] *HCL BigFix Server Version 11.0.3 Detailed Test Report*, Version 1.1, 2025-05-07