National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

PrinterLogic Web Stack Client

Report Number: CCEVS-VR-VID11057-2019
Dated: November 27, 2019
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report 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 for their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the PrinterLogic Web Stack Client 18.3. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of PrinterLogic Web Stack Client was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in November 2019. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 5 and assurance activities specified in *Protection Profile for Application Software, Version 1.3, 1 March 2019* and the *Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019*.

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that PrinterLogic Web Stack Client is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

PrinterLogic Web Stack Client is a product that provides centralized services for user installation of print drivers as well as pull printing and cloud printing functionality.

PrinterLogic Web Stack Client can be used to facilitate direct IP printing. The application interacts with an environmental web server to allow users to install centrally-provisioned printer drivers. It also provides the ability to facilitate pull print jobs that are then released to a selected printer.

PrinterLogic Web Stack Client can also be used for centralized auditing and reporting of print jobs. This allows the organization to identify operational costs based on printer usage so that cost savings can be identified. It also uses SNMP to provide monitoring of individual printers and can generate emails in response to specific SNMP notifications.

PrinterLogic Web Stack is evaluated as a software application only. PrinterLogic Web Stack contains functionality that is not covered by *Protection Profile for Application Software*. As with all evaluations claiming conformance to a NIAP-approved protection profile, only the functionality specified in the ST is evaluated.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	PrinterLogic Web Stack Client version 18.3
Sponsor & Developer	PrinterLogic, LLC 912 West 1600 South St. George, UT 84770
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	November 2019
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
PP	Protection Profile for Application Software, Version 1.3, 01 March 2019 Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of PrinterLogic Web Stack.
Evaluation Personnel	Pascal Patin
Validation Personnel	Jim Donndelinger Patrick Mallett

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 Common Criteria Testing Laboratories (CCTLs) 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 information technology 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).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	PrinterLogic Web Stack Client version 18.3 Security Target
ST Version	1.0
Publication Date	November 27, 2019
Vendor	PrinterLogic
ST Author	Leidos
TOE Reference	PrinterLogic Web Stack
TOE Software Version	18.3
Keywords	Application

2.1 Threats

The ST references the *Protection Profile for Application Software, Version 1.3, 1 March 2019*. No additional threats are defined in the *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019*. The protection profile identifies the following threats, which the TOE and its operational environment are intended to counter:

- 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 communications between the application software and other endpoints in order to compromise it.
- 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.
- 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.
- An attacker may try to access sensitive data at rest.

2.2 Assumptions

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

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

2.3 Organizational Security Policies

There are no Organizational Security Policies defined for the application in the PP.

3 Architectural Information

The section describes the TOE architecture including physical and logical boundaries. Figure 1 shows the TOE in relation to its operational environment.

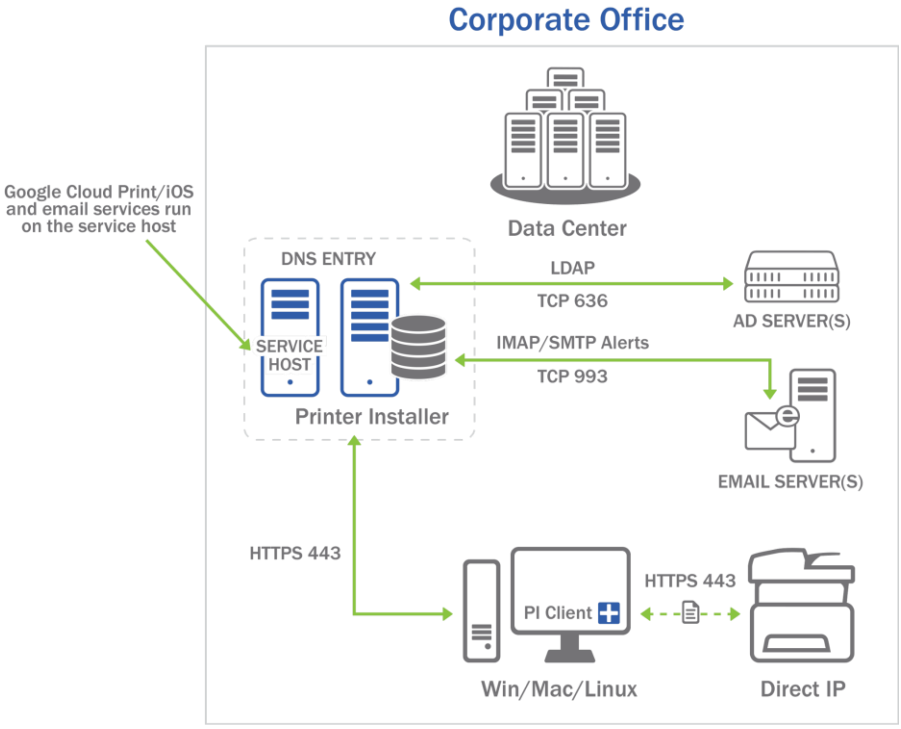

Figure 1 TOE Architecture

The PrinterLogic Web Stack TOE consists of several different components, each of which are standalone applications:

- PL Client (Windows) – a Delphi application with Python components (when configured as Service Host only)
- PL Client (Linux) – a Python application
- PL Client (macOS) – a Python application

Each PL Client component consists of two subsystems: a local printer interface subsystem, which handles installation of print drivers and interfaces between the host platform and an associated server (e.g., to prompt a user to hold or release a pull print job and notify the server if the job is held); and a Service Host subsystem, which allows the PL Client to act as a virtual pull printer to securely retrieve emails and mobile print jobs to be held or released.

4 Clarification of Scope

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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and scoped to those Security Functional Requirements (SFRs) declared in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. The following TOE functionality is specifically excluded in the ST and therefore outside the scope of this evaluation:
    - Installation of print drivers on client PCs.
    - Transmission of print job data from host platforms to target printers or other parts of the TOE operational environment.
    - Configuration of network settings and email servers that allow print data to be received by the TOE.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE uses NIST-validated cryptographic algorithms to secure data in transit. The Windows PL Client application relies on the FIPS-validated cryptographic library cng.sys provided by Windows to perform cryptographic functionality, while the Linux and macOS PL Clients include their own copies of the OpenSSL FIPS Object Module. The Windows PL Client also uses its own instance of OpenSSL-FIPS when running as a Service Host.

The PL Client application (for all platforms) provides TLS/HTTPS client, TLS client, and TLS server functionality. All components rely on their underlying OS platforms to provide entropy used for key generation.

5.2 User Data Protection

The TOE leverages functionality provided by its underlying OS platforms to secure sensitive data at rest. The TOE uses network resources provided by the underlying platforms. The TOE also interfaces with the print spool of its underlying platform. All platform services are invoked with user awareness and authorization.

The TOE uses network connectivity to interact with the Web Server to receive configuration changes and to communicate the status of held print jobs. If configured as a Service host, it will also use network connectivity to securely retrieve print jobs from the operational environment (email server, iOS device, Android device, and/or Google Cloud print server), and to perform reverse AD lookups of users who submit these print jobs.

5.3 Identification and Authentication

The TOE uses X.509 certificates to authenticate endpoints for TLS and HTTPS trusted communications. As with cryptographic functionality in general, the Windows PL Client relies on the operational environment to provide this functionality in some cases while the Linux and macOS PL Clients implement it entirely within the TSF. For all platforms, revocation status is checked using CRLs but connections are authorized if the revocation status of an otherwise valid certificate cannot be confirmed.

5.4 Security Management

PL Client configuration data is stored remotely on the Web Server system. Configuration of the PL Client is performed via administration of the environmental Web Server.

5.5 Privacy

The TOE handles Active Directory credentials as well as print spool data, which could contain personally identifiable information (PII). However, any such handling of data is done with the user's explicit authorization. No transmission of PII occurs that is not in direct response to user activity.

5.6 Protection of the TSF

The TOE includes measures to integrate securely with their underlying OS platforms. The TOE does not perform explicit memory mapping, nor does it allocate any memory region with both write and execute

permissions. Similarly, the TOE does not write user-modifiable data to directories that contain executable files. The TOE is compatible with its supported host OS platforms when those platforms are configured in a secure manner. For all platforms, the TOE is not written in languages that are susceptible to stack-based buffer overflow attacks.

For each supported platform, the TOE uses a well-defined set of platform APIs and third party libraries.

The TOE provides the ability for a user to check its version and to apply updates. Updates are delivered in a format that is appropriate for the TOE's platform (e.g., .deb files for Ubuntu Linux). Application of an update removes all executable code associated with the TOE; there is no way for the TOE to modify its own code. Updates to the TOE are digitally signed, and the signature is validated prior to installation.

5.7 Trusted Path/Channels

TOE components use trusted paths and channels to secure data in transit. The following interfaces are provided by each TOE component:

- PL Client:
    - TLS/HTTPS client for changes to configuration data and pull printing status from Web Server
- PL Client (Service Host only):
    - TLS client for retrieval of print jobs over email (IMAPS)
    - TLS server for retrieval of print jobs over AirPrint (IPPS)
    - TLS client for transmission of printer status data to Google Cloud (XMPP)
    - TLS/HTTPS client for retrieval of print jobs from Google Cloud
    - TLS client for Active Directory communications (LDAPS)

6 Documentation

PrinterLogic provides the following documents that provide information and guidance for the deployment of the TOE:

PrinterLogic Web Stack Client Common Criteria Assurance Activities Report, Version 1.0, 27 November 2019

PrinterLogic Web Stack version 18.3 Common Criteria Supplemental Guidance, Version 1.0, 23 October 2019

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- PrinterLogic Web Stack Client Common Criteria Assurance Activities Report, Version 1.0, 27 November 2019

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Protection Profile for Application Software, Version 1.3, 1 March 2019* and the *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019.*

To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

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.

Testing of the TOE was performed in the summer of 2019 at Leidos's Accredited Test & Evaluation lab.

The evaluators received the TOE in the form that normal 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. For the purposes of testing, the configuration depicted in Figure 2 was used for testing the TOE.

Note that the TOE was tested in conjunction with VID11000. These two products are designed to function together in a production environment, although the TOE was demonstrated to meet all mandatory PP requirements as a standalone product.

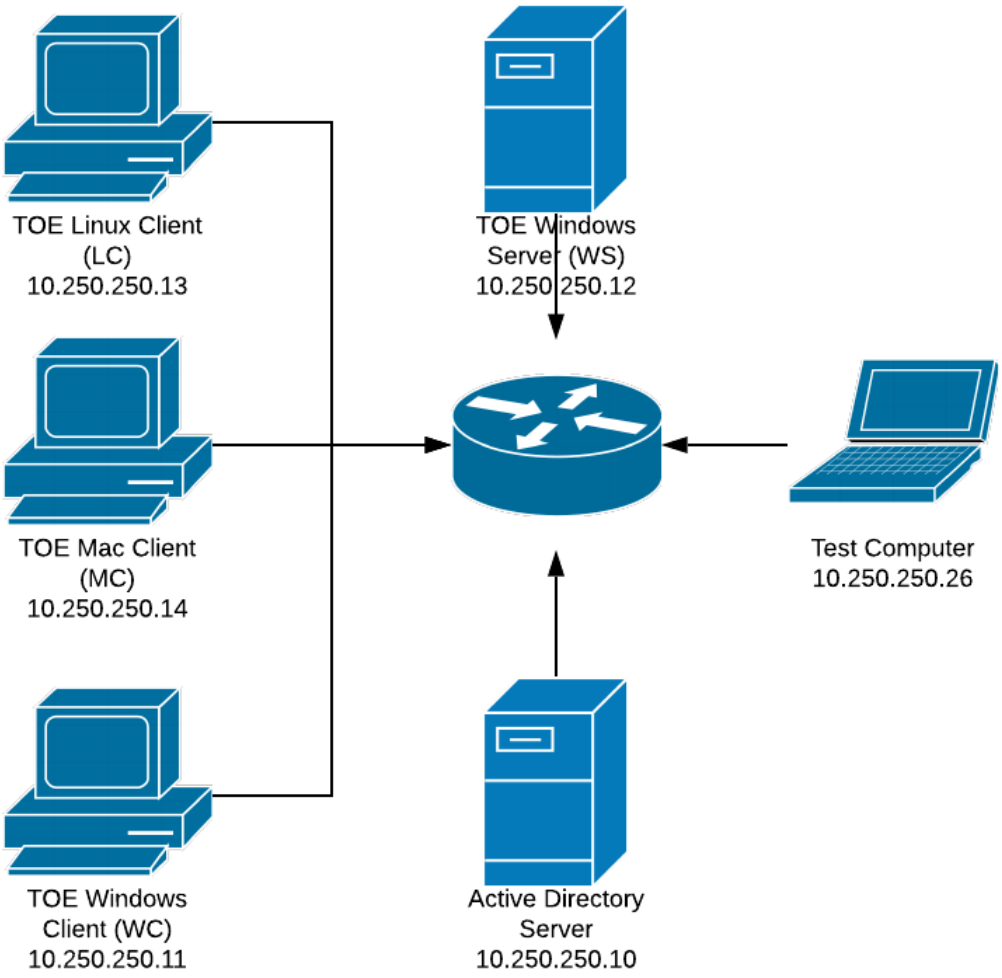

Figure 2 Test Configuration

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

TOE

- PrinterLogic Web Stack Windows Client Component
- PrinterLogic Web Stack Linux Client Component
- PrinterLogic Web Stack Mac Client Component

Additional Components

- PrinterLogic Web Stack Windows Server Component
- Linux Test Computer running the following OS, programs and services:
  - Kali Linux 2019.2 rolling release
  - NIAP provided TLS test server tool, modified by Leidos, updated as of March 1, 2019

  - Leidos TLS test server tool, updated as of March 1, 2019
  - OpenSSL 1.1.0
  - XCA Certificate Authority 1.4.1
  - OpenLDAP 2.4.46
  - Wireshark 2.4.4
- Active Directory Server running Windows Server 2012 R2

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for Application Software, Version 1.3, 1 March 2019* are fulfilled.

7.1 Penetration Testing

The evaluation team conducted an open-source search for vulnerabilities in the product. The evaluator searched the internet for potential vulnerabilities in the TOE using the following sources of the publicly available information:

- http://nvd.nist.gov
- http://www.us-cert.gov
- http://securityfocus.com

The search was conducted using the following terms:

- PrinterLogic
- Printer Installer
- TLS 1.2
- OpenSSL 1.0.2h

Note: In October 2019 PrinterLogic began the process of rebranding their product as PrinterLogic Web Stack which was a change from their old Printer Installer name. A vulnerability search was still conducted on Printer Installer because any vulnerabilities found prior to the fall of 2019 would have been listed under that name. Additionally, a search for PrinterLogic should cover any vulnerabilities listed under PrinterLogic Web Stack.

The search was performed on September 6, 2019 and updated to check for new vulnerabilities on October 22, 2019. The open-source search did not identify any vulnerability applicable to the TOE in its evaluated configuration. No additional testing was required to verify the vulnerabilities were mitigated.

8 Evaluated Configuration

The evaluated version of the TOE is PrinterLogic Web Stack v18.3. The TOE must be deployed as described in section 4 Assumptions of this document and must be configured in accordance with *PrinterLogic Web Stack version 18.3 Common Criteria Supplemental Guidance, Version 1.0, 23 October 2019.*

The following TOE components were installed as part of the evaluated TOE configuration, or as part of a separate PrinterLogic product being evaluated in parallel:

- PrinterLogic Web Stack Windows Server installed on Windows Server 2012 R2
- PrinterLogic Web Stack Windows Client installed on Windows 10
- PrinterLogic Web Stack Linux Client installed on Ubuntu 16.04
- PrinterLogic Web Stack Mac Client installed on Mac OS 10.13

An Active Directory server running Windows Server 2012 R2 and a test computer with penetration testing tools and a TLS test server were also part of the operating environment.

Per NIAP Publication #6 (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf), user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date. The product is still considered by NIAP to be in its evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the *Protection Profile for Application Software, Version 1.3, 1 March 2019* and the *Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019.*

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance Claims
ASE_ECD.1	Extended Components Definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security Objectives
ASE_REQ.1	Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_FSP.1	Basic Functional Specification
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM Coverage
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent Testing – Conformance
AVA_VAN.1	Vulnerability Survey

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 PrinterLogic Web Stack version 18.3 Common Criteria Supplemental Guidance, Version 1.0, 23 October 2019. document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

Name	Description
ST Title	PrinterLogic Web Stack Client version 18.3 Security Target
ST Version	Version 1.0
Publication Date	27 November 2019

13 Abbreviations and Acronyms

AA	Assurance Activity
API	Application Programming Interface
ASLR	Address Space Layout Randomization
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CPA	Control Panel Application
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP(S)	Hypertext Transfer Protocol (Secure)
IP	Internet Protocol
LDAPS	Lightweight Directory Access Protocol Secure
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PL	PrinterLogic Web Stack
PII	Publicly Identifiable Information
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer Protocol
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
XMPP	Extensible Messaging and Presence Protocol

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] *PrinterLogic Web Stack Client version 18.3 Security Target,* Version 1.0, 27 November 2019

[6] *PrinterLogic Web Stack Common Criteria Test Report and Procedures,* Version 1.3, 11 November 2019

[7] *PrinterLogic Web Stack Client version 18.3 Common Criteria Assurance Activities Report,* Version 1.0, 27 November 2019

[8] *PrinterLogic Web Stack version 18.3 Common Criteria Supplemental Guidance Version 1.0,* 23 October 2019