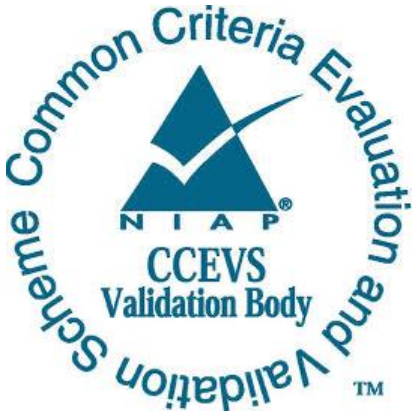
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Imprivata OneSign Version 7.9

Report Number: **CCEVS-VR-VID11178-2023**
Dated: **October 9, 2023**
Version: **1.0**

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

National Security Agency
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel P Faigin
Meredith M Martinez
Mike Quintos
Seada Mohammed
The Aerospace Corporation

Common Criteria Testing Laboratory
King Ables
Travis Hoffmeister
Alejandro Masino
atsec information security corporation, Austin TX

Table of Contents

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Imprivata OneSign Version 7.9 provided by Imprivata, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America, and was completed in October 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both Common Criteria (CC) Part 2 Extended and Part 3 Conformant with a claimed Evaluation Assurance Level of EAL 1 and meets the assurance requirements given in [ESMPMP]:

- Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1

The TOE is Imprivata OneSign Version 7.9 Hot Fix 9 (HF9) (build 7.9.009.58).

The TOE identified in this Validation Report has been evaluated at a NIAP-approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5)" (CC) and the Assurance Activities (AA) of the aforementioned Protection Profile. This Validation Report 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 (CCEVS) 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, reviewed testing activities, 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 the functional requirements and assurance requirements stated in the Security Target (ST). 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 evaluation team concluded that the CC requirements and assurance requirements specified by [ESMPMPP] have been met.

The technical information included in this report was obtained from the Imprivata OneSign Version 7.9 Security Target, Version 1.3.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance 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.

The following table provides information needed to completely identify the product, including the following.

- The Target of Evaluation (TOE): The fully qualified identifier of the product as evaluated
- The ST: Describing the security features, claims, and assurances of the product
- The conformance results of the evaluation
- The Protection Profile (PP) to which the product is conformant
- The organizations and individuals participating in the evaluation

Item	Identifier
Evaluation Scheme	NIAP CCEVS
TOE	Imprivata OneSign Version 7.9 Hot Fix 9 (HF9) (build 7.9.009.58)
PP	Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1
ST	Imprivata OneSign Version 7.9 Security Target (ST), Version 1.3, dated 2023-10-06
ETR	Evaluation Technical Report for a Target of Evaluation Imprivata OneSign Version 7.9, Version 1.3, dated 2023-10-06
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant with a claimed Evaluation Assurance Level of EAL 1
Sponsor	Imprivata, Inc.
Developer	Imprivata, Inc.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Daniel P Faigin, Meredith M Martinez, Mike Quintos, Seada Mohammed

3 Architectural Information

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

OneSign is a policy management product developed by Imprivata, Inc. for managing endpoints in an enterprise. It manages access to endpoint features through the use of policies and provides single sign-on (SSO) capabilities for endpoints. The product consists of two main components:

1. Imprivata Appliance—A virtual appliance (a.k.a. appliance) containing software called OneSign that performs policy management (i.e., the TOE)
2. Imprivata Agent—Agent software (a.k.a. agent) for enforcing policies on endpoints

The TOE is the Imprivata Appliance.

The Imprivata Agents and endpoints reside in the operational environment. The TOE is a single virtual appliance instance running in a VMware ESXi virtual machine. The TOE contains the SUSE Linux Enterprise Server (SLES) OS as its base OS, an Apache HTTP Server, Apache SSHD using Apache Multipurpose Infrastructure for Network Applications (MINA), Java, OpenJDK, and syslog-ng.

In ESM Protection Profile terms, the TOE is a Policy Manager. The Access Control products are the agents located on each endpoint. The TOE is used to create, manage, and provide policies to the enrolled endpoints. The agents enforce the policies on the endpoints.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of Imprivata OneSign Version 7.9 Hot Fix 9 (HF9) (build 7.9.009.58) running as a virtual appliance in a VMware ESXi virtual machine. The following configuration specifics apply to the evaluated configuration of the TOE:

- The TOE is a single virtual appliance instance
- Offline Authentication mode is disabled in the Computer Policies and User Policies
- Only the internal password authentication mechanism is supported (i.e., external authentication servers were not tested)
- Only users in the Imprivata domain are supported
- *Temporary codes for Windows Access* are disallowed
- Apache HTTP Server TLS 1.3 support is disabled
- Network Time Protocol (NTP) is disabled
- File servers for backup functionality are disallowed
- Computer Policy Settings:
    - General » Authentication » “Allow Users to Exit and Disable Agent” is disabled
    - General » Authentication » “Kerberos authentication in place of OneSign authentication” is disabled

  - General » Authentication » “If OneSign authentication fails, but Windows authentication succeeds, should the user be allowed to log in to the computer?” is set to No
  - “Override and Restrict” » “Desktop Access Authentication Restrictions” » “Allow offline authentication” is disabled
- User Policy settings:
  - “Desktop Access authentication” » “Allow offline authentication” is disabled
- The following features were not tested:
  - Fingerprint, Proximity Card, Security Key, Smart Card, USB token, ID token, VASCO OTP, Security Questions, Remote access authentication, OneSign Anywhere authentication, Imprivata ID, Imprivata PIN, Spine Combined Workflow sessions, Self-Service Password, Imprivata Confirm ID, Virtual Desktops, Extensions, Citrix XenApp, Terminal Server, Fast User Switching, ProveID

3.2 Physical Scope of the TOE

The TOE is software and guidance only and is available as a download via the Imprivata website after purchase.

The TOE software (OneSign build 7.9.009.58) consists of the following images:

- 7.9_PROD_G4_OVF.rar
- virtual-applianceG4-IMPRIVATA-2023-2-1.ipm
- virtual-imprivataG4-7-9-9.ipm
- enableAccessControlNIAP-2022-9-12.ipm
- increasePHPmaxPOST-2021-1-22.ipm

The TOE administrative guidance document is the following:

- Imprivata OneSign Version 7.9 Common Criteria Administration Guide

The agent, which is part of the operational environment, is contained in the following download image:

- ImprivataAgent_x64.msi

3.3 Un-evaluated Functionality

The following functions were not evaluated and are, therefore, not included in the secure configuration of the TOE:

- Offline Authentication is not allowed. This mode must be disabled in User Policy
- Temporary codes for Windows Access must be disabled

- Username/password authentication is the only authentication method allowed. This is set by default. Other authentication methods are disabled by default; All other authentication methods cited in Imprivata documentation are forbidden
- Authentication using domain users is not allowed. Only users in an Imprivata domain are allowed
- Imprivata Confirm ID is not allowed
- Apache HTTP Server TLS 1.3 support is disabled
- File servers for backup functionality is disallowed
- Network Time Protocol (NTP) is disabled

4 Security Policy

This section summaries the security functionality of the TOE including the following.

1. Enterprise security management
2. Auditing
3. Cryptographic Support
4. Identification and authentication
5. Security Management
6. Protection of the TSF (TOE Security Functionality)
7. TOE access.
8. Trusted Path/Channels

4.1 Enterprise security management

The TOE supports policy definition and transmission. It allows administrators to define security policies and distribute the policies over a secure connection to the managed endpoints.

The TOE supports the following policies:

- Computer Policy – Capabilities and restrictions placed on the endpoint
- User Policy – Capabilities and restrictions places on the user

The agent combines and enforces the two policies when a user authenticates an endpoint.

4.1.1 Computer Policy

In general, Computer Policies apply to every user attempting to use the endpoint. These policies define the set of features accessible to any user on that endpoint.

The TOE supports the creation (including modification and deletion) of multiple Computer Policies and the application of different Computer Policies to different endpoints. This allows for different Computer Policies to be assigned to different endpoints at any given time.

Computer Policies can control many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware).

The evaluated configuration only tests the following Computer Policy items. (Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit".)

- General
    - Shutdown/restart workstation from lock screen (Select one of: Enable, Disable)
- Walk-Away Security
    - Inactivity detection
        - Keyboard and mouse
            - Lock workstation after (Assignment: Specify time in minutes)
- Override and Restrict
    - Desktop Access Authentication Restrictions
        - Restrict user policy (Select one of: Enable, Disable)
            - Primary Factors
                - Password (Select one of: Enable, Disable)

4.1.2 User Policy

In general, User Policies apply to a specific user attempting to use any endpoint. These policies define the set of endpoint features the user is allowed to use on any endpoint, assuming the endpoint's Computer Policy allows it and the endpoint supports the feature.

The TOE supports the creation (including modification and deletion) of multiple User Policies and the application of different User Policies to different users. This allows for different User Policies to be assigned to different users at any given time.

User Policies can control user access to many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware).

The evaluated configuration only tests the following User Policy items. (Many items in the policy have editable fields that allow an administrator to configure the policy. These editable fields contain the terms: "select", "assignment", and "edit".)

- Authentication
    - Primary Factors
        - Password (Select one of: Enable, Disable)
    - Lockout
        - Lock user account after (Assignment: Specify number of failed attempts) consecutive failures within (Assignment: Specify time in minutes) minutes.
        - Lock account for (Assignment: Specify time in minutes) minutes.

A user policy is assigned to a user by the administrator when the user is initially created. The administrator can later assign a different policy to the user.

It is the agent's responsibility to interpret and enforce the two types of policies. In the areas where the two policies intersect, such as in the area of authentication mechanisms, the agent only uses the features that both policies allow.

4.2 Auditing

The TOE generates audit records for the PP-required events. An administrator can select events to be audited by the TOE based on the event type. The records are protected from unauthorized modification and deletion within the TOE.

The TOE supports two separate mechanisms for storing its audit records externally. Some audit records can be transmitted as individual audit records to an external audit server (a.k.a. syslog server) over a protected communications channel. The remaining audit records can be transmitted in log files to external audit log storage over a protected communications channel.

The TOE allows an administrator to select the events audited by the agent based on event type.

4.3 Cryptographic Support

The TOE employs the HTTPS protocol, SSH (a.k.a. SSHv2) protocol, and TLS protocol to protect communication channels.

The HTTPS protocol is implemented by the Apache HTTP Server. The Apache HTTP Server uses Apache's Network Security Services (NSS) for its TLS implementation. Apache NSS is a software module that implements both the TLS protocol and cryptographic algorithms.

The SSH protocol is implemented using Apache SSHD. Apache SSHD requires Apache MINA which requires the Java Virtual Machine (VM). The Java VM uses a Bouncy Castle software cryptographic module as the cryptographic provider for the Java Secure Socket Extension (JSSE). Apache SSHD uses the JSSE application programming interface (API) to perform its cryptographic operations in the SSH protocol.

The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module that implements both the TLS protocol and cryptographic algorithms.

Table 11: Appliance cryptographic providers

Cryptographic provider	Protocol	Usage
Apache NSS v3.77	HTTPS (TLS 1.2)	Apache HTTP Server
Bouncy Castle v1.68	SSHv2	Java VM (Apache SSHD)
OpenSSL v1.0.2p	TLS 1.2	Syslog-ng

4.4 Identification and Authentication

4.4.1 Admin Console

For the Admin Console, the TOE contains an internal authentication server used to authenticate users. The authentication server uses an internal database to store user data and credentials. The TOE requires the Admin Console users to be identified and authenticated prior to accessing any management functions.

The TOE enforces authentication failure handling on the Admin Console.

The Admin Console supports multiple administrator roles. Administrator roles consist of zero or more administrator role attributes. Multiple administrator roles can be assigned to an administrator. The administrator role attributes of these roles are summed together when the user logs in to the Admin Console to provide the administrator with a complete set of administrator role attributes.

4.4.2 Appliance Console

For the Appliance Console, the TOE uses a separate password file to store and authenticate users. The TOE also enforces authentication failure handling on the Appliance Console.

The Appliance Console supports two administrator accounts: Super Administrator and Administrator. These accounts are used to perform low-level configuration and maintenance.

4.5 Security Management

The TOE supports multiple security management functions required by [ESMPMPP]. These include user account management and policy management functions.

The Admin Console supports two types of administrator roles:

- Super Administrator
- Delegated Administrator

The Super Administrator can perform all administrative functions supported by the Admin Console. A Delegated Administrator can only perform functions delegated to it through the use of administrator role attributes.

The Appliance Console supports the following roles:

- Super Administrator
- Administrator

The Administrator role provides access to a subset of the functionality of the Super Administrator role.

Agents must periodically contact the TOE to receive updated policies and information. The frequency at which the agents contact the TOE is called the Refresh Interval. The Refresh Interval is a global value managed by administrators through the TOE's Admin Console with a value ranging from 3 minutes to 24 hours.

In the OneSign architecture, the TOE never contacts the agents. Instead, the agents contact the TOE under the following conditions:

- At each agent Refresh Interval
- Each time a user attempts to authenticate to and endpoint/agent

4.6 Protection of the TSF

The TOE obscures authentication data before storing them in non-volatile memory. No interface is provided by the TOE to view the passwords in plaintext. Similarly, the TOE provides no interface to view pre-shared keys, symmetric keys, and private keys.

The TOE also provides its own reliable time stamp capabilities.

4.7 TOE Access

The TOE terminates the remote sessions of the Admin Console and Appliance Console after an administrator-configurable time interval of inactivity. It also allows administrators to terminate their own sessions on the Admin Console and Appliance Console (i.e., logout).

The Admin Console and Appliance Console display configurable advisory messages prior to authentication. Depending on which console, administrators can deny session establishment based on day, time, duration, or username.

4.8 Trusted Path/Channels

The TOE acts as an HTTPS server supporting TLS 1.2 when communicating with the agents. Administrators externally manage the TOE using a web browser (i.e., Admin Console and Appliance Console) over HTTPS with TLS 1.2.

The TOE uses the secure copy protocol (SCP) (i.e., SSHv2) to protect the communication channel when transferring audit data from the TOE to external audit log storage.

The TOE uses TLS 1.2 to protect the communication channel when transferring audit data from the TOE to the external audit server (syslog).

Table 22: Appliance secure protocols

Protocol	Initiator
HTTPS (TLS 1.2)	Admin Console to TOE
	Appliance Console to TOE
	Agent to TOE
SSHv2 client	TOE to External audit log storage
TLS 1.2	TOE to External audit server (syslog)

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the associated [ESMPMPP].

- Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1

That information has not been reproduced here, and the respective documents should be consulted if there is interest in that material. Additionally, the Security Problem Description has been presented in the Security Target.

5.1 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the ST and the associated the PP.

Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the device 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 clarification. This text covers some of the more important limitations and clarifications of this evaluation.

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 [ESMPMPP]) performed by the evaluation team.

Specific exclusions from this evaluation are described in the subsection Un-evaluated Functionality in Section 3.

6 Documentation

The following documentation was used as evidence for the evaluation of the TOE.

- Imprivata OneSign Version 7.9 Common Criteria Administration Guide, September 12, 2023 [CCGUIDE]

Any additional customer documentation delivered with the product or that may be available through download was not included in the scope of the evaluation and, hence, should not be relied upon when configuring or using the products in the evaluated configuration.

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 configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. The specific test configurations and test tools utilized may be found in the Assurance Activity Report (AAR) in Section 2.3.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

7.2.1 Test Approach

Testing was performed at atsec CCTL. No testing required assistance that can only be provided by the developer, and the evaluator was able to perform all tests. All required Assurance Activities specified by [ESMPMPP] were tested by the evaluator.

7.2.2 Test Configuration

The developer provided the necessary software and documentation so that the evaluator could configure the TOE in the evaluated configuration.

The test system was set up according to a setup strategy that followed the evaluated configuration requirements specified in the guidance, supplemented by configurations required to perform testing.

The test platform consists of a Dell PowerEdge R740xd 2U Rack Server with Intel Xeon Gold 5222 (Cascade Lake), running a hypervisor (VMware ESXi 6.7 Update 3) containing the TOE appliance.

In addition to the TOE platform, a VMware ESXI system hosting two virtual machines are used in the testing:

1. A server VM #1 running CentOS 8 hosting SSH and OpenSSL
2. A client VM #2 running CentOS 8 hosting the Imprivata agent

The following software tools were used to support the testing activities:

1. Wireshark 3.6.8
2. Tcpdump 4.9.3
3. Nmap 7.70
4. OpenSSL 1.1.1k

7.2.3 Test Results

Results are summarized in the Assurance Activity Report (AAR) and fully described in the proprietary Detailed Test Report.

8 Evaluated Configuration

The guidance documentation specified in Section 6 provides specific instructions for configuring the Enterprise settings for the TOE to comply with the functions defined in the Security Target.

8.1 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

All work units defined by CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the [ESMPMPP] received a pass verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements as well as assurance activities. The evaluation was conducted based upon CEM Version 3.1 Revision 5. The evaluation determined the TOE to be CC Part 2 extended and Part 3 compliant and to meet the assurance requirements defined by the [ESMPMPP].

8.2 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit and the assurance activity specified in [ESMPMPP]. The ST evaluation ensured that the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Imprivata OneSign Version 7.9 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the Imprivata OneSign Version 7.9 and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Development Documentation (ADV)

The evaluation team applied each ADV CEM work unit and assurance activity specified in [ESMPMPP]. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification were 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.

8.4 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit and assurance activity specified in [ESMPMPP]. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both the administrator and user 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 were provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM and the PP and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and assurance activity specified in [ESMPMPP]. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer can identify the evaluated TOE.

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

8.6 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit and assurance activity specified in [ESMPMPP]. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed/devised an independent set of tests as mandated by the protection profile.

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

8.7 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit and assurance activity specified in the [ESMPMPP]. The vendor provided security updates to the TOE during the evaluation; therefore, while the tested version of the TOE did contain vulnerabilities, subsequent security updates, in line with the guidance provided in Scheme Policy Letter 15, fixed all known issues. The evaluation team ensured that the currently available version of the TOE does not contain known exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis and the evaluation team's performance of penetration tests.

The evaluators searched for publicly known vulnerabilities applicable to the TOE using the following sources. The search was performed on multiple occasions as follows:

- 2022-11-10
- 2023-02-06
- 2023-06-02
- 2023-07-05
- 2023-07-25
- 2023-08-31
- 2023-09-13

In addition, the evaluation team used the following public sources:

- Common Vulnerabilities and Exposures (CVE)
  https://cve.mitre.org/index.html
- Cybersecurity and Infrastructure Security Agency (CISA)
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- OpenSSL website
  https://www.openssl.org/news/vulnerabilities.html

using the following search terms:

- Imprivata OneSign
- Apache HTTP server
- Apache web server
- Apache httpd
- Apache MINA
- Apache Multipurpose Infrastructure for Network Applications
- Apache Network Security Services
- Apache NSS
- Mozilla NSS
- Apache SSHD
- Apache Tomcat
- Bouncy Castle

- BouncyCastle
- Java Virtual Machine
- Java VM
- Java Secure Socket Extension
- Java JSSE
- jvm
- log4j
- OpenJDK
- OpenSSL
- Oracle Database
- Oracle DBMS
- PHP
- spring framework
- spring mvc
- SLES
- SUSE Linux Enterprise Server
- syslog-ng
- TLS 1.2

The evaluator's CVE search found no vulnerabilities applicable to the TOE or that affect the security of the TOE in the evaluated configuration.

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

8.8 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of the testing defined by PP and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator’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 PP and correctly verified that the product meets the claims in the ST.

9 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 document listed in Section 6. No other 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 needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable.

11 Security Target

Imprivata OneSign Version 7.9 Security Target, Version 1.3, dated 2023-10-06.

12 Glossary

The following definitions are used throughout this document.

AA	Assurance Activity
AES	Advanced Encryption Standard
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory—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.
CEM	Common Criteria Evaluation Methodology
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
ETR	Evaluation Technical Report
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.
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
RFC	Request For Comments

SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation—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.
TLS	Transport Layer Security
TSF	TOE Security Functionality
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.
VR	Validation Report

13 Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1
- Imprivata OneSign Version 7.9 Common Criteria Administration Guide, 2023-09-12
- Imprivata OneSign Version 7.9 Security Target, Version 1.3, 2023-10-06
- Imprivata OneSign Version 7.9 Assurance Activity Report, Version 1.3, 2023-10-06
- Imprivata OneSign Version 7.9 Evaluation Technical Report, Version 1.3, 2023-10-06
- Imprivata OneSign Version 7.9 Evaluation Technical Report, Assurance Class AVA, Version 1.1, 2023-09-13
- Imprivata OneSign Version 7.9 Detailed Test Report, Version 1.0, 2023-10-04