National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report
General-Purpose Operating System Protection Profile, Version 3.9

Report Number: CCEVS-VR-PP-0014
Dated: 20 January 2015
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Leidos (formerly SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the General-Purpose Operating System Protection Profile (version 3.9), which is also referred to as GPOSPP. It presents a summary of the GPOSPP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the GPOSPP was performed concurrent with the first product evaluations against the PP's requirements. In this case the Targets of Evaluation (TOEs) for these first evaluations were *Microsoft Windows 8*[1] *and Windows RT* and *Microsoft Windows 8*[2] *and Windows Server 2012* provided by Microsoft Corporation. The evaluations were performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America. The CCTL completed the evaluations in January 2015. The information in this report is largely derived from the Evaluation Technical Reports (ETRs) written by the CCTL.

The evaluation determined that the GPOSPP is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 4). Because the ST contains only material drawn directly from the GPOSPP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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 found that the evaluation showed that the GPOSPP meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

[1] Windows 8 Edition
[2] Windows 8 Pro and Windows 8 Enterprise Editions

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the GPOSPP was performed concurrent with the first product evaluations against the PP. In this case the TOEs for these first evaluations were the *Microsoft Windows 8*[3] *and Windows RT* and *Microsoft Windows 8*[4] *and Windows Server 2012* provided by Microsoft Corporation. The evaluations were performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America. The CCTL completed the evaluations in January 2015.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the initial evaluations performed against this PP.

Protection Profile	*General-Purpose Operating System Protection Profile*, Version 3.9, 15 January 2013
PP Evaluation Technical Report	*Protection Profile Evaluation Technical Report for General-Purpose Operating System Protection Profile*, Version 1.0, 15 January 2015
ST	*Microsoft Windows 8 and Windows RT Security Target*, Version 1.0, 19 December 2014.
ST	*Microsoft Windows 8 and Windows Server 2012 Security Target*, Version 1.0, 19 December 2014.
ST Evaluation Technical Report	*Security Target Evaluation Technical Report For Microsoft Windows 8, Windows RT and Windows Server 2012*, Version 5.6, 17 June 2014
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 4, September 2012
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCEVS Validators	Ken Elliott, The Aerospace Corporation

[3] Windows 8 Edition
[4] Windows 8 Pro and Windows 8 Enterprise Editions

3 GPOSPP Description

This GPOSPP defines the security functionality expected to be provided by a general-purpose operating system capable of operating in a networked environment. The GPOSPP covers general-purpose operating systems that provide a multi-user and multi-tasking environment. It also provides a set of assurance components that define the minimum set to be used in an evaluation of an operating system for compliance with this Protection Profile. GPOSPP defines the general approach and assurance activities required to be performed during the evaluation, thereby refining the stated assurance components.

The main purpose of a general-purpose operating system (from a security point of view) is to provide defined objects, resources and services to entities using the functions provided by the operating system at its external interfaces, and to enforce a defined policy on access to objects, use of resources, and use of services. At a minimum, the operating systems addressed by GPOSPP export interfaces to programs executing "on top of" the operating systems and interfaces to external entities, including network interfaces, as well as interfaces to devices that are used to "transport" data or actions of external entities to the operating system (for example, a keyboard and a mouse). In addition, the operating system uses functions of the underlying hardware and software to provide its functions, including using devices that are not connected to an external entity such that this entity could affect the behavior of the device directly (for example, hard disks or displays).

An operating system conformant to GPOSPP can be operated as a server system within a data center, but also as a client system used directly by one or more human users. While it is mandatory that an operating system conformant to GPOSPP must be capable of providing and using some basic network services, such a system may also be started in an environment where it is not connected to any network and with the network services inactive. It is mandatory that an operating system conformant to GPOSPP must provide basic security functionality for user identification and authentication, access control, management and audit.

A GPOSPP TOE will provide user services directly or serve as a platform for networked applications, and will support protected communication using one or more cryptographically-protected network protocols or the support of dedicated, physically-separated network links. To support protected communication, a GPOSPP TOE must implement at least the TCP/IP network protocol family; GPOSPP makes no statements about the version of IP.

GPOSPP addresses general-purpose operating systems operating in a well-managed enterprise environment. This addresses mostly servers, but also desktop clients if their operating environment fulfills the security problems defined in the profile. See below section 4 Security Problem Description and Objectives. These security problems include requirements for professional management of the system and basic protection against physical attacks that can be found in enterprise or government environments, but typically not in home environments

administered by private users. The enterprise or government environments may include setups for mobile systems or home-offices provided that the TOE implements mechanisms that allow these environments to comply with the security problem definition in GPOSPP. GPOSPP makes no claims or statements that it specifically applies to either a server operating system or a client operating system. If an operating system meets the requirements defined in the security problem definition of the GPOSPP base, with or without any extended packages, the operating system can claim conformance to GPOSPP.

4 Security Problem Description and Objectives

The specific conditions listed in the following subsections are assumed to exist in a GPOSPP TOE's Operational Environment. The security objectives counter the identified threats and satisfy the defined policies and assumptions.

4.1 Assumptions

These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
A.DETECT	Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
A.PEER.MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
A.PEER.FUNC	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
A.CONNECT	All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.2 Threats

The following threats are addressed by GPOSPP base-conformant TOEs. GPOSPP covers these threats to derive the necessary security functionality.

Table 2: Threats

Threat Name	Threat Definition
T.ACCESS.TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the necessary authorization.
T.ACCESS.USERDATA	A threat agent may gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy by using functions provided by the TOE.
T.ACCESS.TSFFUNC	A threat agent may use or manage functionality of the TSF bypassing protection mechanisms of the TSF.
T.ACCESS.COMM	A threat agent may access cryptographically protected data transferred via a trusted channel between the TOE and another remote trusted IT system, modify such data during transfer in a way not detectable by the receiving party or masquerade as a remote trusted IT system.
T.RESTRICT.NETTRAFFIC	A threat agent may send data packets to the recipient in the TOE via a network communication channel in violation of the information flow control policy.
T.IA.MASQUERADE	A threat agent may masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA.USER	A threat agent may gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated by the TSF.
T.UNATTENDED_SESSION	A threat agent may gain unauthorized access to an unattended session.

4.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. GPOSPP defines these organizational security policies to derive the necessary security functionality.

Table 3: Organizational Security Policies

Policy Name	Policy Definition

Policy Name	Policy Definition
P.ACCOUNTABILITY	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has.

4.4 Security Objectives

This subsection describes the security objectives of the GPOSPP. GPOSPP includes both security objectives for the TOE and objectives for the operational environment.

Table 4: Security Objectives for the TOE

Objective Name	TOE Security Objective Definition
O.AUDITING	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The TSF must protect this information and present it to authorized users if the audit trail is stored on the local system. The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.DISCRETIONARY.ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.NETWORK.FLOW	The TOE shall mediate network communication between an entity outside of the TOE and a recipient within the TOE in accordance with its network information flow security policy.
O.SUBJECT.COM	The TOE shall mediate any possible sharing of objects or resources between subjects acting with different subject security attributes in accordance with its discretionary access control policy
O.I&A	The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to be provided to authenticated users only.

Objective Name	TOE Security Objective Definition
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
O.TRUSTED_CHANNEL	The TSF must allow authorized users to remotely access the TOE using a cryptographically-protected network protocol that ensures integrity and confidentiality of the transported data and is able to authenticate the end points of the communication. Note that the same protocols may also be used in the case where the TSF is physically separated into multiple parts that must communicate securely with each other over untrusted network connections. The protocol must also prevent masquerading of the remote trusted IT system.
O.UNATTENDED_SESSION	The TOE must allow for the temporary suspension of a user's session allowing the continuation of such a suspended session and user related input and output only after the user has resumed the session by re-authenticating himself to the TSF.

Table 5: Security Objectives for the Operational Environment

Objective Name	Environment Security Objective Definition
OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide the functions required by the TOE and are sufficiently protected from any attack that may cause those functions to provide false results.

Objective Name	Environment Security Objective Definition
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: ▪ All network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted. ▪ DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. ▪ Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
OE.INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
OE.MAINTENANCE	Authorized users of the TOE must ensure that the comprehensive diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
OE.RECOVER	Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (security) compromise is achieved.
OE.TRUSTED.IT.SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are under the same management domain as the TOE, are managed based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

5 Requirements

As indicated in section 3, GPOSPP is structured into a "base" part and a set of (optional) "extended packages". Extended packages are not yet explicitly defined in GPOSPP[5]. Table 6 lists the security functional requirements covered in this GPOSPP evaluation.

Table 6: GPOSPP Security Functional Requirements

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.1: Protected Audit Trail Storage
	FAU_STG.3: Action in Case of Possible Audit Data Loss
	FAU_STG.4: Prevention of Audit Data Loss
FDP: User Data Protection	FDP_ACC.1: Complete Access Control
	FDP_ACF.1: Security Attribute Based Access Control
	FDP_IFC.1: Subset Information Flow Control
	FDP_IFF.1: Simple Security Attributes
	FDP_RIP.2: Full Residual Information Protection
FIA: Identification & Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_ATD.1: User Attribute Definition for Individual Users
	FIA_UAU.1(RITE): Timing of Authentication
	FIA_UAU.1(HU): Timing of Authentication
	FIA_UAU.5: Multiple Authentication Mechanisms
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UID.1: Timing of Identification
	FIA_USB.1: User-Subject Binding
	FIA_PK_EXT.1: Public Key Based Authentication

[5] The first product evaluation included additional security functional requirements drawn from class FCS for cryptographic services. These FCS requirements were not covered in the protection profile evaluation of GPOSPP.

Requirement Class	Requirement Component
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MSA.1: Management of Security Attributes
	FMT_MSA.3(DAC): Static Attribute Initialization
	FMT_MSA.3(NI): Static Attribute Initialization
	FMT_MSA.4: Static Attribute Value Inheritance
	FMT_MTD.1(AE): Management of TSF Data
	FMT_MTD.1(AS): Management of TSF Data
	FMT_MTD.1(AT): Management of TSF Data
	FMT_MTD.1(AF): Management of TSF Data
	FMT_MTD.1(CM): Management of TSF
	FMT_MTD.1(NI): Management of TSF Data
	FMT_MTD.1(IAT): Management of TSF Data
	FMT_MTD.1(IAF): Management of TSF Data
	FMT_MTD.1(IAU): Management of TSF Data
	FMT_REV.1(OBJ): Revocation for Object Access
	FMT_REV.1(USR)): Revocation for Object Access
	FMT_SMF_RMT.1: Remote Management Capabilities
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_STM.1: Reliable Time Stamps
FTA: TOE Access	FTA_SSL.1: TSF-initiated Session Locking
	FTA_SSL.2: User-initiated Locking
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel

6 Assurance Requirements

Table 7 lists the security assurance requirements claimed in GPOSPP.

Table 7: GPOSPP Security Assurance Requirements

Requirement Class	Requirement Component
ASE: Security Target	ASE_INT.1: ST introduction
	ASE_CCL.1: Conformance claims
	ASE_SPD.1: Security problem definition
	ASE_OBJ.2: Security objectives
	ASE_ECD.1: Extended components definition
	ASE_REQ.2: Derived security requirements
	ASE_TSS.1: TOE summary specification
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.3: Authorisation controls
	ALC_CMS.3: Implementation representation CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.3: Systematic flaw remediation
	ALC_LCD.1: Developer defined life-cycle model
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: basic design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2: Vulnerability analysis

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

7.1 Errata

These errata detail changes that correct errors in version 3.9 of GPOSPP.

1. P.ROLES is absent from GPOSPP Table 4: Security policies sufficiency, Table 1: Coverage of security objectives for the TOE, and Table 2: Coverage of security objectives for the TOE environment. The table entries are:
   Table 1:

O.MANAGE	P.ACCOUNTABILITY, P.USER, P.ROLES, T.ACCESS.TSFFUNC

   Table 2:

OE.ADMIN	P.ROLES, A.AUTHUSER, A.MANAGE, A.TRAINEDUSER

   Table 4:

P.ROLES	The policy to match the trust given to an administrator and restrictions on actions the administrator is given authority to perform is implemented by: • OE.ADMIN requiring trustworthy personnel managing the TOE and • O.MANAGE allowing appropriately-authorized administrators restricted authority to manage the TSF.

2. O.UNATTENDED_SESSION is absent from GPOSPP Table 7: Security Functional Requirements coverage and Table 8: Security Functional Requirements rationale. The table entries are:
   Table 7:

FTA_SSL.1	O.I&A, O.UNATTENDED_SESSION
FTA_SSL.2	O.I&A, O.UNATTENDED_SESSION

Table 8:

O.UNATTENDED_SESSION	User-initiated and TSF-initiated session locking [FTA_SSL.1, FTA_SSL.2] provided the capability to suspend and resume an interactive session with re-authentication required to resume.

3. The first selection in FMT_MTD.1.1(AT) should include the option 'none':
   FMT_MTD.1.1 The TSF shall restrict the ability to **modify, [selection: add, delete, none]** the **actions to be taken in case of audit storage failure …**

7.2 Security Assurance Requirements Verdicts

Table 8 reproduces the security assurance requirement verdicts from GPOSPP protection profile ETR.

Table 8: Protection Profile Evaluation Verdicts

APE Requirement	Evaluation Verdict
APE_INT.1	Pass
APE_CCL.1	Pass
APE_SPD.1	Pass
APE_OBJ.2	Pass
APE_ECD.1	Pass
APE_REQ.2	Pass

8 Glossary

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the GPOSPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model,* Version 3.1, Revision 4, September 2012

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements,* Version 3.1, Revision 4, September 2007

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements,* Version 3.1, Revision 4, September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security: Evaluation Methodology,* Version 3.1, Revision 4, September 2012

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security. *Guidance to Validators of IT Security Evaluations, Scheme Publication #3,* Version 1.0, January 2002

[6] OSPP Technical Community. *General-Purpose Operating System Protection Profile,* Version 3.9, 15 January 2013

[7] Leidos, Inc. *Protection Profile Evaluation Technical Report for General-Purpose Operating System Protection Profile,* Version 1.0, 15 January 2015

[8] Leidos, Inc. *Security Target Evaluation Technical Report For Microsoft Windows 8, Windows RT and Windows Server 2012,* Version 5.6, 17 June 2014