Supporting Document
Mandatory Technical Document

PP-Module for Widgets

Version: 1.0

2020-01-16

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be "Guidance Documents", that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or "Mandatory Technical Documents", whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2016-10-06	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Widgets products.

Acknowledgements:
This SD was developed with support from NIAP Widgets Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the Widgets PP-Module is to describe the security functionality of Widgets products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Protection Profile for Network Devices, Version 2.1

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Widgets, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activites to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'. To reach a 'fail' verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a 'pass'. To reach a 'fail' verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

The following sections list Common Criteria and technology terms used in this document.

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common	Common Criteria for Information Technology Security Evaluation (International Standard

Criteria (CC)	ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.3.2 Technical Terms

Access Point (AP)	A device that provides the network interface that enables wireless client hosts to access a wired network.
End User Device (EUD)	A device that has the ability to process, transmit, and/or store information.
Service Set Identifier (SSID)	The primary name associated with an 802.11 wireless local area network (WLAN).
Wireless Intrustion Detection System (WIDS)	A security product that provides network security administrators with the ability to monitor, collect, and log real-time to potentially malicious wireless (IEEE 802.11) network traffic.
Wireless Intrustion Prevention	A security product that provides network security administrators with the ability to monitor, collect, log, and react in real-time to potentially malicious wireless (IEEE

System (WIPS)	802.11) network traffic.
Wireless Local Area Network (WLAN)	A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM work units that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for Network Devices

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the ND PP.

2.1.1 Modified SFRs

2.1.1.1 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

2.1.1.2 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_ARP.1 Security Alarms

FAU_ARP_EXT.2 Security Alarm Filtering

FAU_GEN.1/WIDS Audit Data Generation

FAU_GEN_EXT.1 Intrusion Detection System – Reporting Methods

FAU_IDS_EXT.1 Intrusion Detection System – Intrusion Detection Methods

FAU_INV_EXT.1 Environmental Inventory

FAU_INV_EXT.2 Characteristics of Environmental Objects

FAU_INV_EXT.3 Behavior of Environmental Objects

FAU_INV_EXT.4 Location of Environmental Objects

FAU_SAA.1 Potential Violation Analysis

FAU_WID_EXT.1 Wireless Intrusion Detection – Malicious Environmental Objects

FAU_WID_EXT.2 Wireless Intrusion Detection – Passive Information Flow Monitoring

FAU_WID_EXT.3 Wireless Intrusion Detection – Denial of Service

FAU_WID_EXT.4 Wireless Intrusion Detection – Unauthorized Authentication Schemes

FAU_WID_EXT.5 Wireless Intrusion Detection – Unauthorized Encryption Schemes

2.2.2 User Data Protection (FDP)

FDP_IFC.1 Information Flow Control Policy

2.2.3 Security Management (FMT)

FMT_SMF.1/WIDS Specification of Management Functions (WIDS)

2.3 Evaluation Activities for Optional SFRs

2.3.1 Security Audit (FAU)

FAU_WID_EXT.6 Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring

FAU_WID_EXT.7 Wireless Intrusion Detection – Wireless Spectrum Analysis

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Security Audit (FAU)

FAU_ANO_EXT.1 Anomaly-Based Intrusion Detection

FAU_SIG_EXT.1 Signature-Based Intrusion Detection

FAU_STG_EXT.1/PCAP Protected Audit Event Storage (Packet Captures)

2.5 Evaluation Activities for Objective SFRs

2.5.1 Security Audit (FAU)

FAU_INV_EXT.5 Detection of Unauthorized Connections

FAU_INV_EXT.6 Signal Library

FAU_MAC_EXT.1 Device Impersonation

FAU_WIP_EXT.1 Wireless Intrusion Prevention

2.5.2 Protection of the TSF (FPT)

FPT_FLS.1 Basic Internal TSF Data Transfer Protection

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the ND PP base to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The ND PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP

and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.