Supporting Document
Mandatory Technical Document

PP-Module for Host Agent

Version: 1.0

2020-01-31

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	2020-01-31	Draft - first version released

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

Acknowledgements:
This SD was developed with support from NIAP Host Agent 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 Host Agent PP-Module is to describe the security functionality of Host Agent products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the Application Software Protection Profile.

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for Host Agent, Version 1.0. 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 .
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
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	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	A comprehensive set of security requirements for a product type that consists of at least one

Configuration	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 a ST.
Target of Evaluation (TOE)	The product under evaluation.

1.3.2 Technical Terms

Endpoint	A computing device that runs a general purpose OS, mobile device OS, or network device OS. Endpoints can include desktops, servers, and mobile devices.
Endpoint Detection and Response (EDR)	A system that analyzes collected EDR Host Agent data for detecting, investigating, and remediating unauthorized activities on endpoints.
Enrolled State	The state in which an endpoint with a running Host Agent is managed by an ESM. Also, referred to as Onboarding.
Enrollment	The process of transitioning an endpoint from an unenrolled to an enrolled state.
Enterprise Security Management (ESM)	A enterprise security management application hosted on a server or cloud service that provides support for security management, information flows, reporting, policy, and data analytics in complex enterprise environments.
Host Agent	A logical piece of software that executes on endpoints to collect data about the endpoint and executes commands sent to the endpoint from an Enterprise Security Management (ESM) server or service. An example command sent to an endpoint could be to enforce a policy from an ESM, to collect some files, or to run an OS command.
Operating System (OS)	Software that manages physical and logical resources and provides services for applications.
Unenrolled State	The state in which an endpoint, with or without a Host Agent, is not managed by an ESM. Also, referred to as Offboarding.

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 6 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 cPP.

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 Application Software Protection Profile

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

2.1.1 Modified SFRs

2.1.1.1 User Data Protection

FDP_NET_EXT.1 Network Communications

TSS
The TSS is unchanged from the Base-PP.
Guidance
The guidance is unchanged from the Base-PP.
Tests
The tests are unchanged from the Base-PP.

2.1.2 TOE SFR Evaluation Activities

2.1.3 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation (Refined)

TSS
The evaluator shall verify the TSS lists all record types that are recorded.

The evaluator shall verify that the TSS lists all the auditable event types and all audit information that the TOE records.
Guidance
The evaluator shall check the administrative guide and ensure that it lists all of the auditable events. The evaluator shall check to make sure that every audit event type selected in the ST is included.

The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall ensure that the fields contains the information required.
Tests

- **Test 1:** The evaluator shall test the Host Agent's ability to correctly generate audit records by having the Host Agent generate audit records for each type of event listed in the ST.
- **Test 2:** The evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record provide the required information.

FAU_STO_EXT.1 Audit Data Storage

TSS
The evaluator shall verify the TSS contains details of where all audit data is stored.
Guidance
The evaluator shall check the administrative guide and ensure that the list of auditable events are stored in the platform provided logging mechanism.
Tests

- **Test 1:** The evaluator shall test the Host Agent's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. This should include all instance types of an event specified. When verifying the test results, the evaluator shall ensure the audit records generated during testing are stored in the platform provided logging mechanism.
  On Linux based platforms this would be in var/logs. On Windows based platforms this would be the Windows Event Log. No specific locations are defined for other platforms.

2.1.4 Host Agent (FHA)

FHA_HAD_EXT.1 Host Agent Declaration

TSS
The evaluator shall verify the TSS lists all classes of products the Host Agent is designed to function with.

Guidance
The evaluator shall check the administrative guide and ensure that guidence exists for enrollment with all compatible ESM products identified in the ST.
Tests

- **Test 1:** Conditional: If EDR is selected the evaluator shall install the Host Agent and enroll it with the EDR management system. The evaluator shall verify that enrollment was successful and that the Host Agent is communicating with the EDR.

2.1.5 Security Management (FMT)

FMT_SMF.1/1 Specification of Management Functions (Configuration of Host Agent)

TSS
The evaluator shall verify the TSS contains all frequencies for sending Host Agent data to an ESM and all labels that are permitted.
Guidance
The evaluator shall verify that every management function mandated by the PP-Module is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Tests

- **Test 1:** The evaluator shall test the ability to configure the Host Agent and test each option from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

FMT_UNR_EXT.1 User Unenrollment Prevention

TSS
The evaluator shall ensure that the TSS describes the mechanism used to prevent users from unenrolling the Host Agent.
Guidance
There is no associated guidance for this requirement.
Tests

- **Test 1:** The evaluator shall attempt to unenroll the Host Agent from the ESM system as an unprivileged user and verify that the attempt fails, by trying to kill the process or stop the Service or Daemon that is running the Host Agent.

3 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

4 Evaluation Activities for Selection-Based SFRs

4.1 Host Agent (FHA)

FHA_CHA_EXT.1 Cache Host Agent Collected Data

TSS
The evalutator shall verify the TSS details how data is cached, any rules that would effect data caching, and how cached data will be effected if storage limit are reached.
Guidance
The evalutor shall verify that any configuration options related to data caching is listed in the guidance.
Tests

- **Test 1:** The evaluator shall test the Host Agents ability to cache data by disconnecting the endpoint from the network for a period of 72 hours to simulate a network connectivity failure, these should be actual hours not via changing system time. The evaluator shall exercise behaviors on the endpoint during the 72 hour time frame to generate Host Agent data. Example behaviors could be running programs, performing some authentications, installing/uninstalling software, or sample test cases provided by the vendor to generate Host Agent data. The evaluator will then reconnect the endpoint to the network and verify on the ESM system that the missing data from the 72 hour time frame is available on the ESM management portal.

FHA_COL_EXT.1 Collected Audit

TSS
The evaluator shall verify the TSS contains a full list of endpoint data that can be collected.
Guidance
The evaluator shall check the administrative guide and ensure that it lists all of the collectable types of endpoint event data.

The evaluator shall check to make sure that every endpoint event type listed in the ST is included in the administrative guidance.
Tests
The evalutator shall run the systems causing multiple events to occur then review the items collected by the Host Agent and verify all items in the minimum set are included.

4.2 Trusted Path/Channels (FTP)

FTP_DIT_EXT.2 Protection of Data in Transit for Peer-to-Peer Host Agents

TSS
The evaluator shall verify that the TSS contains a description of all data transmitted to other Host Agents and that all such data is protected by according to FPT_DIT_EXT.1.
Guidance
The evaluator shall ensure the guidance contains any configuration details required for ensuring data transmitted to other Host Agents is protected by TLS.
Tests

- **Test 1:** The tests in FTP_DIT_EXT.1.1 shall be repeated for data trasmitted between two Host Agents.

5 Evaluation Activities for Objective SFRs

5.1 Security Management (FMT)

FMT_POL_EXT.1 Trusted Policy Update

TSS
The evaluator shall ensure that the TSS describes how the candidate policies or commands are sent to the Host Agent; the processing associated with verifying the digital signature of the policies or commands; and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluators (this could be the Host Agent or the underlying platform).
Guidance
There is no associated guidance for this requirement.
Tests

- **Test 1:** The evaluator shall perform or wait for a policy update or commands from an ESM Server to be sent to a Host Agent. The evaluator shall verify the policy or command is signed and is provided to the Host Agent. The evaluator shall verify the Host Agent accepts the digitally signed policy.

  The execution of this test may require some configuration or a test version of either the Host Agent of the ESM system in order to view the incoming policy or command and verify that the content is digitally signed.
- **Test 2:** The evaluator shall alter a policy update or command and verify the Host Agent rejects the altered policy.

6 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the App 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 App 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.

7 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.
[AppPP]	Protection Profile for Application Software
[EDR]	Protection Profile for Endpoint Detection and Response