Supporting Document
Mandatory Technical Document

PP-Module for Redaction Tools
Version: 1.0-Draft
2022-04-29
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-Draft	2022-04-29	Initial publication

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

Acknowledgments:
This SD was developed with support from NIAP redaction tools 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 PP-Module for Redaction Tools is to describe the security functionality of redaction tools 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 Application Software, version 1.4

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

- redaction tools, Version 1.0-Draft

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities 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.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard 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.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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-PPs.
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.
Target of Evaluation (TOE)	The product under evaluation.
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.

1.3.2 Technical Terms

Attachments	An electronic document or data file that is part of the main file but is logically distinct and separable from the main electronic document.
Complex Objects	Objects that may have their own static or functional metadata and may differ between the stored and visible form, such as images, attachments, Microsoft OLE objects, Microsoft ActiveX controls, and temporal objects.
Functional data	Forms, scripts, link Uniform Resource Locators (URLs), workflow data, action buttons, formulas in a spreadsheet, macros or any type of executable content.
Images	The actual image data stored in the file as opposed to what is visible; the visible image can be cropped or resized but the full image could still be retained in the file format and may or may not match the visible image; some image formats can have their own metadata, such as Joint

	Photographic Experts Group (JPG) and Tagged Image File Format (TIFF).
Metadata of objects or embedded objects	Data associated with an object to describe or identify the contents of the object such as exchangeable image file format (EXIF) data of images; images themselves can contain other images and their own metadata.
Obscured visible data	Content that could be visible but is obscured in some way such as content that runs off an edge of the container, text in a black font on black background (or any color of font on a similar color background), very small fonts, cropped or clipped graphics or images, hidden layers, portions of an embedded object (e.g. Microsoft Object Linking and Embedding (OLE)) that are outside the view container.
Remnant data	Artifacts of the original application or source file format such as remnant or unreferenced data from fast saves, unreferenced or unused elements, malformed elements that cannot be fixed, garbage data in the file structure.
Static data or metadata	File properties such as author or creation date, stored form field data, undo cache or any data kept to revert to a prior version of an element or the document itself, incremental updates, collaboration data such as comments, tracked changes, workflow data, embedded search indexes, bookmarks, document info added by 3rd-party apps, accessibility data such as alternate text, etc.
Structural data	Data that is part of the file format structure, such as a file header or fonts, and is necessary to interpret the file properly for display or print.
Temporal Objects	A particular type of complex object whose representation extends through a time interval, such as video, audio, flash animation, slide shows, etc. References to “complex objects” in the requirements section of this paper include temporal objects.
Visible contents	The visual representation of text, images, and complex objects in a file.

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 workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled 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 workunit 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 workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled 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 workunits 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 Application Software

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

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the Application Software PP is the base.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_ALR_EXT.1 Redaction Failure Notification

FAU_ALR_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes how the TOE notifies the user when redaction fails. The evaluator shall ensure that the TSS' description complies with the requirement that the user is notified when redaction fails for any reason.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall acquire or create test files that should fail the redaction, use the TOE to attempt the redaction process with the expectation of its failure, and verify that the TOE alerts the user that the redaction failed.

FAU_REP_EXT.1 Report Generation

FAU_REP_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes the TOE's reporting feature and the metadata that is included for each report entry.

Guidance
The evaluator shall examine the operational guidance to ensure it contains instructions for the configuration of the reporting feature in accordance with this requirement.

Tests
The evaluator shall create test files with specific elements to redact, apply the TOE to the test files, and observe that there is a report for each element expected to be redacted. This assurance activity can be done in conjunction with FAU_SAR_EXT.1.

FAU_SAR_EXT.1 Report Review

FAU_SAR_EXT.1
TSS
There are no TSS EAs for this component.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create test files with specific elements to redact, apply the TOE to the test files, and observe that there is a report entry for each element expected to be redacted.

2.2.2 User Data Protection (FDP)

FDP_DID_EXT.1 Identification of Data

FDP_DID_EXT.1.1
TSS
The evaluator shall examine the TSS to ensure it specifies the hidden data that it identifies and allows the user to select for redaction. The evaluator shall ensure that the TSS' description complies with the requirement for the TOE to identify all hidden data and allow the user to review and select each hidden data element for redaction.

Guidance
There are no guidance EAs for this element.

Tests
The evaluator shall create test documents with various types of hidden data apply the TOE, and verify that it identifies each expected element and allows the user to select and redact each.
FDP_DID_EXT.1.2
TSS
The evaluator shall examine the TSS to ensure it describes how the TOE handles all obscured data. The evaluator shall ensure that the TSS' description complies with the requirement that all obscured data is identified and either removed automatically or redacted by the user.

Guidance
There are no guidance EAs for this element.

Tests
The evaluator shall create test documents with various forms of obscured data, apply the TOE, and verify that the tool identifies the obscured data and either removes the obscured data automatically or gives the user the

choice to remove or retain the obscured data.
FDP_DID_EXT.1.3
TSS
There are no TSS EAs for this element.

Guidance
There are no guidance EAs for this element.

Tests
The evaluator shall create a test document with an image that is stored in a larger size and resolution than the visible image and apply the TOE without selecting the image for redaction. The evaluator shall verify that the TOE either:

- Gives the user a choice to retain the image unaltered or replace the stored data with the visible data. For the choice to replace the image, the evaluator shall examine the output file to locate the image and verify its size and resolution, or extract the image with an appropriate tool for that format and compare the size and resolution of the extracted image to the visible image to determine if they match.
- Resizes the stored image. To determine this, the evaluator shall examine the output file to locate the image and verify its size and resolution, or extract the image with an appropriate tool for that format and compare the size and resolution of the extracted image to the visible image to determine if they match.

FDP_DIN_EXT.1 Deep Inspection

FDP_DIN_EXT.1
TSS
The evaluator shall examine the TSS to ensure it lists and describes the methods used to replace redacted elements that contain metadata, other elements, or hidden data. The evaluator shall ensure that the TSS' description complies with the requirement that each element is handled by either recursing through the element chain and applying the TOE to each layer, simplifying the element, or redacting the element.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files that contain elements that themselves contain other elements and hidden data. The evaluator shall examine the document to identify these elements in the structure, apply the TOE, and examine the output to verify that the elements were handled properly via either redaction or simplification in accordance with the requirement.

FDP_LOC_EXT.1 Redact Content from Every Location

FDP_LOC_EXT.1
TSS
There are no TSS EAs for this component.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files that contain content in multiple places and examine the files to locate the content. The evaluator shall apply the TOE and examine the output to verify that it has been removed from every location.

FDP_NND_EXT.1 No New Data Introduced by TOE

FDP_NND_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes the actions taken by the TOE when removing, simplifying, or redacting an element. If structural data is added, the TSS shall specify what structural data is added and the purpose of the structural data. If non-structural hidden data is added, the TSS shall detail the added hidden data and describe how the user is notified of the addition. The evaluator shall ensure that the TSS' description complies with the requirement to not introduce new hidden data, other than structural data, without warning the user.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files with complex objects or other elements and examine the files to locate those items in the structure. The evaluator shall use the TOE to perform the redaction operation and examine the output to verify that no new hidden data or metadata was introduced.

FDP_OBJ_EXT.1 Removal of Objects and Corresponding References

FDP_OBJ_EXT.1
TSS
The evaluator shall examine the TSS to ensure its description of the removal of redacted objects includes the removal of all references and indicators to the redacted objects in conformance with the requirement.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files that contain objects and examine the files to locate these objects in the file format and all references to them in the structural data. The evaluator shall apply the TOE and select elements for complete redaction. The evaluator shall examine the output files to verify that the objects and all references to them have been redacted.

FDP_REM_EXT.1 Removal of Redacted Data

FDP_REM_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes the removal of all data selected for redaction and verify that no encryption, encoding, or proprietary process is used to obscure selected data. The evaluator shall ensure that the TSS' description complies with the requirement to remove all data selected by the user or identified by the TOE for redaction.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall acquire or create test files that contain text, images, and other elements. The evaluator shall examine the test files to locate the content in the format. The evaluator shall apply the TOE, marking some of the content for redaction, and examine the output to verify that the marked content was removed and not obscured through encryption, encoding, or conversion to a proprietary format.

FDP_RIP_EXT.1 Residual Information Removal

FDP_RIP_EXT.1
TSS
The evaluator shall examine the TSS to ensure it specifies the residual data and objects (e.g., remnant data, undo buffers, tracked changes buffers, multiple versions of the same object, and any buffer or cache type data container) that the TOE will remove from files without any user interaction. The evaluator shall ensure that the TSS' description complies with the requirement to automatically remove all such data.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files that contain the types of data described in the requirement and examine the files to locate the data. The evaluator shall apply the TOE and not select anything for redaction, and examine the files to verify that this data has been removed automatically.

FDP_RPL_EXT.1 Visible Space Replace

FDP_RPL_EXT.1
TSS
The evaluator shall examine the TSS to ensure it lists and describes the content used to replace redacted elements. The evaluator shall ensure that the TSS' description complies with the requirement to convey no information about the previous contents.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire a test file with an image, mark part of the image for redaction and apply the TOE, and examine the image in the output to verify that the visual appearance does not provide any indication of the content that was redacted. If the TOE allows text content to be replaced with text, the evaluator shall create or acquire a test file with some text as content, apply the TOE, and verify that the replacement text does not preserve word length or other identifying information that could allow recovery of the original content.

FDP_SEL_EXT.1 Selected Redaction

FDP_SEL_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes in detail which complex objects can be simplified by the TOE and how they are simplified (e.g., whether the object or the whole page is converted to another

format and what that format is). The TSS shall also list those complex objects or images that cannot be simplified and will be removed.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test documents that contain complex objects and examine the documents to identify where those objects are in the format. The evaluator shall then apply the TOE and examine the output to verify that the objects have been simplified or removed. The evaluator shall test all objects that can be simplified as well as all objects that should be removed according to the TSS.

The evaluator shall also create or acquire test documents with complex objects that are not documented in the TSS, apply the TOE, and verify that those objects are removed from the document.

FDP_VAL_EXT.1 Validation of Data

FDP_VAL_EXT.1.1
TSS
There are no TSS EAs for this element.

Guidance
There are no guidance EAs for this element.

Tests
The evaluator shall create or acquire test files that contain unrecognized data, unexpected data, and extraneous structural data. The evaluator shall examine the files prior to redaction to identify the data. The evaluator shall apply the TOE but make no visible redactions and save the output files. The evaluator shall examine the output files, comparing it to the originals, to verify that the data has been removed.
FDP_VAL_EXT.1.2
TSS
The evaluator shall examine the TSS to ensure that it describes how the TOE handles data that it cannot completely interpret.

Guidance
There are no guidance EAs for this element.

Tests
The evaluator shall create or acquire test files with data that the TOE should not be able to completely interpret, apply the TOE and examine the output to verify that the TOE handled the data according to the requirement.

2.2.3 Security Management (FMT)

FMT_RVW_EXT.1 Element Review

FMT_RVW_EXT.1
TSS
There are no TSS EAs for this component.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create test documents that contain images, text, and complex objects, use the TOE to perform the redaction operation, and verify that each element is selectable for redaction in whole or in part.

2.2.4 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1
TSS
The evaluator shall examine the TSS to ensure it describes what actions the TOE performs upon any failure. The evaluator shall ensure that the TSS’ description complies with the requirement to not produce a partially redacted file.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall create or acquire test files that cause the TOE to fail and observe that the TOE fails and does not produce partially redacted files.

2.3 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.4 Evaluation Activities for Selection-Based SFRs

The PP-Module does not define any selection-based requirements.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base Application Software PP 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 Application Software 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.
[App PP]	Protection Profile for Application Software, Version 1.4, October 2021