Application Software Extended Package for Redaction Tools

Version: 2.0
2015-12-11
National Information Assurance Partnership

Revision History

Version	Date	Comment
v 1.0	2014-05-14	Final Version 1.0 Released
v 1.1	2015-06-16	Interim Draft - Update as Extended Package of the Protection Profile for Application Software

Contents

1. Introduction

1.1 Overview

The scope of this Extended Package (EP) is to describe the security functionality of Redaction tools in terms of [CC]. Redaction is the process of selectively removing and replacing information from a document or other logical container of data for release to an audience not intended to view that information. Redacted information is not limited to classified material; other examples include privacy data, proprietary information, trade secrets, and legal strategy. Instances of redaction include replacing classified text with a black box to release a document to an unclassified environment, replacing privacy-related data such as telephone numbers with all Xs to release a database to a contractor, converting a proprietary format document to Portable Document Format (PDF) to release a what-you-see-is-what-you-get (WYSIWYG) document. The risk from improper or incomplete redaction is the inadvertent disclosure of classified or sensitive data.

Redaction is not sanitization. In the sanitization process, information is removed with no indication that the sanitization process took place. In the redaction process, selected visible information is removed and replaced with something innocuous (e.g. black box or text) so that the reader knows redaction took place. This replacement is a critical part of the process not shared with sanitization.

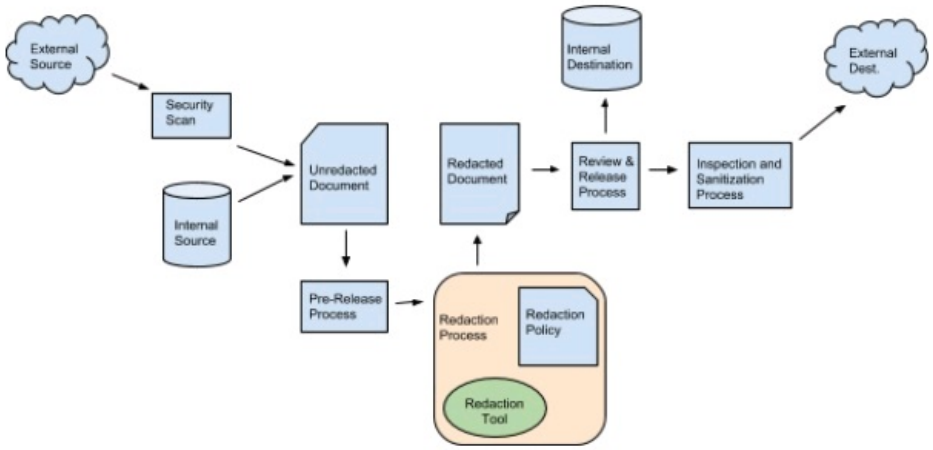

Figure 1: One possible workflow of an electronic document through the redaction process.

Figure 1 shows the typical workflow of a document from source to destination and through the redaction process. Other workflows are possible. Software vendors have the flexibility to devise their own workflow solutions for their target consumer. However, in any workflow, this protection profile applies only to the part of the workflow that is performed by the redaction tool and only to the redaction functionality in that tool. Other functionality in the redaction tool, other tools used in the workflow, the organization's redaction policy as well as security requirements and security policies that apply to other parts of the workflow are beyond the scope of this protection profile.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this Extended Package.

1.2.1 Common Criteria Terms

Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Extended Package (EP)	An implementation-independent set of security requirements for a category of products, which extends those in a Protection Profile.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation. In this case, application software and its supporting documentation.
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.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.

1.2.2 Technology Terms

Visible contents	The visible contents of the file; the visual representation of text, images and complex objects.
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 OLE) that are outside the view container.

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.
Functional data	Forms, scripts, link Uniform Resource Locators (URLs), workflow data, action buttons, formulas in a spreadsheet, macros or any type of executable content.
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.
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).
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.
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.
Metadata of objects or embedded objects	Such as EXIF data of images; images themselves can contain other images and their own metadata
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.

1.2.3 Other Terminology

The following concepts are used in the assurance activities.

Simplify (or simplified)	Replace a complex object or element with a single layer element that does not contain hidden or obscured data. The original representation of the object and all of the original hidden data must be removed from the document and the visible space must be replaced with the simplified element. For example, a document could contain an embedded spreadsheet on a page where only a small portion of the spreadsheet is visible within the view container on the page while content in the rest of the spreadsheet is in the document but hidden from the viewer. To simplify such an object, the TOE could create a single layer image (with no metadata of its own) from just the portion of the spreadsheet that is visible, place that image on the page and remove the embedded spreadsheet. This is just one solution. The intent of simplifying an object is to remove something complex that could contain hidden data and replace it with something simple that does not contain hidden data.
Examine a test file or document	The evaluator uses a hex editor or similar tool to view the raw binary (or hex) data of the file and the format structure. This allows the evaluator to view the contents of the file directly rather than through the TOE’s interpretation of those contents. The examination can include the use of tools to extract, decode or decompress certain types of elements from the format, such as text or images. Care must be taken so that the extraction process does not change the element’s size, resolution, or content. The Technical Community will identify appropriate tools.
Apply the TOE	Follow the multi-step process where the user selects or marks areas or items in a document for redaction and then instructs the TOE to redact the marked areas and hidden information from the file.
Test files	To test the TOE, the evaluator will have to use test documents that have content expected to produce a certain result. The evaluator will apply the redaction tool to the test files and examine the output to determine if it is as expected. The same test documents can be used for each TOE that produces the same format as those test documents. For example, a set of PDF test files can be used for all PDF redaction tools. Test files will usually contain only one testable item at a time to make it easier to identify that item in the structure of the document, but some test files should contain multiple testable items. The Technical Community will create a set of test files for the assurance activities for the most common formats.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this EP is a redaction application running on a desktop or mobile operating system.

This EP describes the extended security functionality of a redaction tool in terms of [CC]. As an extension of the App PP, it is expected that the content of this EP will be appropriately combined with the App PP to include selection-based requirements in accordance with the selections and/or assignments made, and any optional and/or objective components to include: FCS_CKM.2.1, FCS_COP.1.1(*), FCS_RBG_EXT.2.*, FCS_TLSC_EXT.1.*, FIA_X509_EXT.1.*, FIA_X509_EXT.2.*.

An ST must identify the applicable version of the App PP and this EP in its conformance claims.

This EP is limited to the redaction of electronic documents defined in standards such as the series International Organization for Standards (ISO)/International Electrotechnical Commission (IEC)-29500 (Office OpeneXtensible Markup Language (XML), e.g. Microsoft Word, PowerPoint, and Excel documents) and ISO/IEC-32000 (PDF), or the definitive standard for a format. Mail guards, filters, and batch redaction tools are beyond the scope of this EP.

Requirements that apply to features such as administrative control over particular redaction settings, multi-person review prior to release, etc., are outside the scope of this EP. The TOE may have those features but is not required to have them and their use and enforcement is governed by the organization’s redaction policy.

This EP covers the software functionality of the redaction process; it does not include requirements for how users should decide what to redact or other policy issues. Analysis of documents for covert data transfer is part of the decision-making process for what to redact and so occurs prior to the redaction itself. The requirements in this document are independent of requirements levied on document release by statute or the judiciary.

Data execution risks inherent in some file formats are beyond the scope of this EP. This EP assumes that scanning for such risks occurs prior to the document entering the redaction functionality of the TOE.

Documents to be redacted may contain objects that are vulnerable to steganography, such as images or video. Functional data such as scripts can contain strings or images that may not be accessible to the redaction tool. Analysis of such objects for attacks or covert data transfer will occur outside of the redaction process. An organization’s security policy will determine whether such objects are released or redacted in their entirety.

1.4 Use Cases

Redaction Tools perform tasks associated primarily with the following use case.

[USE CASE 1] Content Redaction

Redaction Tools are used for the redaction of user selected content from a document.

2. Conformance Claims

Conformance Statement

The Protection Profile for Application Software ([AppPP]) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for application software products. This EP serves to extend the App PP baseline with additional SFRs and associated Assurance Activities specific to redaction tools. Assurance Activities are the actions that the evaluator performs in order to determine an email client's compliance to the SFRs.

This EP conforms to Common Criteria [CC] for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant. In order to be conformant to this EP, the ST must include all components in this EP and the associated App PP that are:

- unconditional (which are always required)
- selection-based (which are required when certain selections are chosen in the unconditional requirements)

and may include optional and/or objective components that are desirable but not required for conformance.

In accordance with CC Part 1, dependencies are not included when they are addressed by other SFRs. The assurance activities provide adequate proof that any dependencies are also satisfied.

3. Security Problem Description

The security problem is described in terms of the threats that the redaction tool is expected to address, assumptions about the operational environment, and any organizational security policies that it is expected to enforce.

This Extended Package does not repeat the threats, assumptions, and organizational security policies identified in the *Protection Profile for Application Software* (App PP), though they all apply given the conformance and hence dependence of this EP on it. Together the threats, assumptions and organizational security policies of the App PP and those defined in this EP describe those addressed by a redaction tool as the Target of Evaluation.

3.1 Threats

The following threats are specific to redaction tools, and represent an addition to those identified in the App PP.

T.CLUES_TO_ORIGINAL_DATA
Text or graphics placed in the redacted area by the TOE may contain clues to the nature of the original redacted information.

T.UNREDACTED_DATA
A failure of the redaction tool to remove user selected visable or hidden data could reuslt in the inadvertant dissemination of information.

3.2 Assumptions

This section of the security problem definition shows the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality.

A.KNOWLEDGEABLE_USER
The user is knowledgeable concerning document management and has appropriate training with the redaction tool. Part of this knowledge and training includes how to prepare a document for the redaction tool, e.g. resolve and turn off tracked changes prior to redaction, work with a copy of the document and preserve the original file, remove passwords and decrypt files, etc.

A.INFORMATION_RELEASE_POLICY
There is a redaction or information release policy in place for the organization which the user follows.

A.PRESERVE_DOCUMENT_LAYOUT
The TOE will preserve the layout of the document.

4. Security Objectives

This Extended Package adds SFRs to objectives identified in the App PP and describes an additional objective specific to this EP.

O.INSPECTION
The TOE will analyze the file content for metadata and elements, to include any that are purposely hidden or not immediately visible to the naked eye. This metadata and elements includes, but is not limited to those that are obstructed from view such as shapes on top of text, hidden objects (manual direct formatting or programmatically hidden), and text that is positioned off the margins, and/or is located in header and footer sections of the file.
Addressed by: RED_DIN_EXT.1, RED_ID_EXT.1

O.MANAGEMENT
Addressed by: RED_RVW_EXT.1

O.QUALITY
Addressed by: VAL_REM_EXT.1, RED_NND_EXT.1, FPT_FLS.1

O.REDACTION
The TOE will provide the capability to completely remove any data selected for redaction.
Addressed by: RED_SEL_EXT.1, RED_RPL_EXT.1, RED_REM_EXT.1, RED_LOC_EXT.1, RED_OBJ_EXT.1, RED_RIP_EXT.1

O.REPORT

The TOE will provide the capability to produce a report of all data redacted and any errors during redaction.

Addressed by: REP_GEN_EXT.1, REP_RVW_EXT.1, RED_ALR_EXT.1

5. Security Requirements

This chapter describes the security requirements which have to be fulfilled by the redacion tool. Those requirements comprise functional components from Part 2 of [CC]. The following notations are used:

- **Refinement** operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: are identified with a number inside parentheses (e.g. "(1)")

5.1 Security Functional Requirements

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

5.1.1 Report Generation and Review

REP_GEN_EXT.1 Report Generation

REP_GEN_EXT.1.1

The TOE must be able to generate a report entry that contains metadata about each element that was redacted, including at least the following: the type of the element that was removed, the location if it was a visible element, and whether the element was selected by the user or removed automatically.

Application Note: The report can be a configurable feature that is only generated on user request. Location can be a page number, a cell number for a spreadsheet, or some other indication that allows the user to easily locate the visible element.

Assurance Activity

> *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. The evaluator shall examine the operational guidance to ensure it contains instructions for the configuration of the reporting feature in accordance with this requirement. 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 REP_RVW_EXT.1.*

REP_RVW_EXT.1 Report Review

REP_RVW_EXT.1.1

The TOE must allow the user to access a report of the data that was redacted.

Application Note: This can be satisfied with a dialog box or other simple list of items that were redacted. The report can be a configurable feature that is only generated on user request.

Assurance Activity

> *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.*

5.1.2 Validation Stage

VAL_REM_EXT.1 Validation of Data

VAL_REM_EXT.1.1

The TOE must remove unrecognized data, unexpected data, and extraneous structural data.

Application Note: Structural data is extraneous if it is unnecessary for the printing or display of the document contents, or unnecessary for the functionality of the document.

Example - many formats include comments, e.g. PDF allows file format comments which are preceded by %. When these comments are unnecessary, unrelated to the printing or display of the content of the document, or provide no functionality whatsoever they must be removed.

Example – some formats expect a header structure starting at the first byte of a file, but a tool may be able to interpret a file where the header starts at a later byte by ignoring the data that precedes the header structure. In this case, the preceding data must be removed since it is unexpected.

Assurance Activity

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.

VAL_REM_EXT.1.2

The TOE must [**selection**: *simplify*, *remove*] any element which it cannot completely interpret.

Application Note: For example, if the tool cannot recurse through a stream with embedded OLE objects, it must convert the stream to a single layer image with no metadata or remove it. If the redaction tool cannot interpret or process temporal objects, it must remove the temporal object and replace it with a simplified object or other placeholder. If a stream of data is compressed, encoded or encrypted and the redaction tool cannot uncompress, decode or decrypt the data, the tool must delete the stream.

Assurance Activity

The evaluator shall examine the TSS to ensure that it describes how the TOE handles data that it cannot completely interpret. 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.

5.1.3 Redaction Stage

RED_SEL_EXT.1 Selected Redaction

RED_SEL_EXT.1.1

The TOE must [**selection**: *simplify*, *remove*] any complex object, embedded object or graphic image which is selected for redaction.

Application Note: The selection may be of either the whole element or only part of the element. If part of an element is selected, only that part must be simplified or removed.

Assurance Activity

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. 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.

RED_DIN_EXT.1 Deep Inspection

RED_DIN_EXT.1.1

For each element of the file format that can contain its own metadata, other elements, or hidden data, the TOE must [**selection**:

recurse through the element chain and apply the PP to each layer ,
simplify the element,
redact the element

] .

Application Note: For example, JPG images can contain metadata called exif data. Some image formats can contain the same image in another format, such as raw which can contain a complete jpg version of the image. A complex object can contain other complex objects (e.g. Microsoft OLE). The tool must apply the requirements to each layer of every element and identify hidden/metadata not just at the top layer of the document but in each element and in all layers within that element. If the TOE cannot recurse through the layers, it must simplify the element at the top level.

Assurance Activity

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. 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.

RED_RPL_EXT.1 Visible Space Replace

RED_RPL_EXT.1.1

The TOE must replace the visible space of redacted content in such a way that the visible space conveys no information about the previous contents.

Application Note: A vendor may use several different methods to replace content, such as opaque blocks, text, whitespace or some other vendor-defined method. These methods must not convey information about the content being replaced. For example, if text is replaced with text, the replacement text must not indicate length of component words. Blocks of color used to replace parts of images must not show variations in intensity that could convey information about the image content.

Assurance Activity

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. 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.

RED_REM_EXT.1 Removal of Redacted Data

RED_REM_EXT.1.1

All data that is either selected by the user for redaction or identified by the TOE for redaction must be removed from the document.

Application Note: Selected content must be removed, not obscured by encryption, encoding, conversion to a proprietary format, or any other method.

Assurance Activity

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. 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.

RED_LOC_EXT.1 Redact Content from Every Location

RED_LOC_EXT.1.1

The TOE must remove redacted content from every location in the file format where it is stored.

Assurance Activity

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.

RED_NND_EXT.1 No New Data Introduced by TOE

RED_NND_EXT.1 .1

The TOE itself must not introduce new hidden data that was not requested by the user without warning the user of the addition.

Application Note: If the redaction process changes the format of an object, such as converting a complex object to an image, the conversion must not introduce new metadata.

The TOE can modify or add structural data, including fonts, without alerting the user if the modification is necessary for the proper display or print of the file.

Assurance Activity

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. 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 examiner shall apply the TOE and examine the output to verify that no new hidden/metadata was introduced.

RED_OBJ_EXT.1 Removal of Objects and Corresponding References

RED_OBJ_EXT.1.1

The TOE must remove all references and indicators in the structural data to objects that are completely redacted by the TOE.

Application Note: In some formats, there are references in the structural data to objects, such as a name dictionary in PDF. If an object in a PDF document, such as an image, is completely redacted (i.e. the user has selected the entire image to be redacted), then not only must the image data be removed, but references to it in a name dictionary as well as all structural references to the image must be removed. If only part of the object is selected for redaction, then the references necessarily remain in the file since the object remains in the file.

Assurance Activity

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. 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.

RED_RIP_EXT.1 Residual Information Removal

RED_RIP_EXT.1.1

The TOE must automatically remove all remnant data, undo buffers, tracked changes buffers, multiple versions of the same object, and any buffer or cache type container of data.

Application Note: The user does not have to select this data for removal.

Assurance Activity

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. 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.

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [assignment: any failure].

Application Note: If the redaction functionality fails for any reason, the TOE must not produce a partially redacted file.

Assurance Activity

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. 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.

5.1.4 User Experience

User Experience

RED_ID_EXT.1 Identification of Data

RED_ID_EXT.1.1

The TOE must identify all hidden data in the document, except remnant data and undo or tracked change buffers, and allow the user to review and select each hidden data element individually for redaction.

Application Note: Remnant data and undo or tracked change buffers are removed automatically according to RED_RIP_EXT.1. If the file or part of the file is encrypted, the TOE will have to reject the file or decrypt it so that the tool and the user can review the hidden data.

Assurance Activity

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. 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.

RED_ID_EXT.1.2

The TOE must identify all obscured data and must [**selection**:

remove the obscured data automatically,

allow the user to redact the obscured data

] .

Application Note: Obscured data is anything that could be visible but is obscured in some way, such as the cropped portion of an image or graphic. While the user sees only the portion of the graphic in the view container, the document contains the data in the cropped area. The tool must either remove the obscured data automatically or give the user the choice to remove or retain the obscured area.

Assurance Activity

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. 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.

RED_ID_EXT.1.3

The TOE must identify images where the visible representation is reduced in size or resolution from the representation stored in the file format and must [**selection**:

automatically replace the stored data with the visible representation,

allow the user to replace the stored data with the visible representation,

allow the user to leave the image unaltered

] .

Assurance Activity

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.

RED_RVW_EXT.1 Element Review

RED_RVW_EXT.1.1

The TOE must allow the user to review and select each element of visible data in whole or in part for redaction.

Application Note: If the file or part of the file is encrypted, the TOE will have to reject the file or decrypt it so that the user can review the data.

Assurance Activity

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

RED_ALR_EXT.1 Redaction Failure Notification

RED_ALR_EXT.1.1

The TOE must make the user aware when redaction fails for any reason.

Assurance Activity

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. The evaluator shall acquire or create test files that should fail the redaction, apply the TOE and verify that the TOE alerts the user that the redaction failed.

A. Optional Requirements

As indicated in Section , the baseline requirements (those that must be performed by the TOE) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C. The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this PP. The second type (in Appendix B) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this EP, so adoption by vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

B. Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the browser or its underlying platform) are contained in the App PP and in the body of this EP. There are additional requirements based on selections from the App PP and/or in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

C. Objective Requirements

This Annex includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this EP as they describe security functionality not yet widely-available in commercial technology. However, these requirements may be included in

the ST such that the TOE is still conformant to this EP, and it is expected that they be included as soon as possible.

D. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[AppPP]	Protection Profile for Application Software