Requirements from the *Application Software Extended Package for Redaction Tools*

Version: 2.0

2015-12-11

National Information Assurance Partnership

Revision History

Version	Date	Comment

Introduction

Purpose. This document presents simplified view of the functional and assurance requirements found in the *Application Software Extended Package for Redaction Tools*. Common Criteria evaluation, facilitated in the U.S. by the National Information Assurance Partnership (NIAP), is required for IA and IA-enabled products in National Security Systems according to CNSS Policy #11.

Using this document. This representation of the Protection Profile includes:

- *Security Functional Requirements* for use in evaluation. These are featured without the formal Assurance Activities specified in the Protection Profile, to assist the reader who is interested only in the requirements.

  It also includes, in tables shown later, particular types of security functional requirements that are not strictly required in all cases. These are:

  - *Selection-based Security Functional Requirements* which become required when certain selections are made inside the regular Security Functionality Requirements (as indicated by the **[selection:]** construct).
  - *Objective Security Functional Requirements* which are highly desired but not yet widely-available in commercial technology.
  - *Optional Security Functional Requirements* which are available for evaluation and which some customers may insist upon.

- *Security Assurance Requirements* which relate to developer support for the product under evaluation, development processes, and other non-functionality security relevant requirements.

Security Functional Requirements

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.

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.

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.

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.

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.

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.

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.

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.

RED_LOC_EXT.1.1 The TOE must remove redacted content from every location in the file format where it is stored.

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.
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.
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.
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.
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.
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.
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*] .
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.
RED_ALR_EXT.1.1	The TOE must make the user aware when redaction fails for any reason.

Security Assurance Requirements

Selection-Based Security Functional Requirements

Objective Security Functional Requirements

Optional Security Functional Requirements