

Supporting Document

Mandatory Technical Document



PP-Module for Web Browsers

Version: 2.0

2015-06-16

National Information Assurance Partnership

Foreword

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

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

Technical Editor:

National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
v 1.0	2014-03-31	Release - Protection Profile for Web Browsers
v 2.0	2015-06-16	Update as Extended Package of the Protection Profile for Application Software
v 2.0	2015-06-16	Application Software Extended Package for Web Browsers
v 1.0	2014-03-31	Initial release - Protection Profile for Web Browsers

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of Web Browsers products.

Acknowledgements:

This SD was developed with support from NIAP Web Browsers 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
 - 1.2 Structure of the Document
- 2 Evaluation Activities for SFRs
 - 2.1 TOE SFR Evaluation Activities
 - 2.2 Evaluation Activities for Optional SFRs
 - 2.3 Evaluation Activities for Selection-Based SFRs
 - 2.4 Evaluation Activities for Objective SFRs
- 3 Evaluation Activities for SARs
- 4 Required Supplementary Information

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Web Browsers is to describe the security functionality of Web Browsers products in terms of [CC] and to define functional and assurance requirements for them.

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.

2 Evaluation Activities for SFRs

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

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

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

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

2.1 TOE SFR Evaluation Activities

The PP-Module does not define any mandatory requirements (i.e. Requirements that are included in every configuration regardless of the PP-Bases selected).

2.2 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.3 Evaluation Activities for Selection-Based SFRs

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

2.4 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-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 the Base-PP as well. The Base-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 chosen 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-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