Supporting Document
Mandatory Technical Document

PP-Module for Web Browsers
Version: 1.0
2021-06-18
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	2021-06-18	Initial release as PP-Module

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

Acknowledgments:
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

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. 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 :

- Web Browsers, Version 1.0

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	A Protection Profile developed by international technical communities and approved by

Protection Profile (cPP)	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.
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

Add-on	Capabilities or functionality added to an application. This term includes plug-ins, extensions, and other controls.
Administrator	The Administrator is responsible for management activities, including setting the policy that is applied by the enterprise on the browser. This administrator is likely to be acting remotely. If the platform is unmanaged by an enterprise, the user can act as the administrator.
Cross-Site Request	A vulnerability where an attacker gets a target user to execute a script with that user's

Forgery (CSRF)	privileges.
Cross-Site Scripting (XSS)	Injection of untrusted content into a vulnerable web application to render or execute that content on a victim's system.
Domain	A realm of administrative autonomy, authority or control on the internet (e.g., cnn.com).
Extension	A bundle of code added to the browser to add specific functionality that the browser does not provide by default.
HTML5	A new version of HTML that incorporates many new features that enrich the browsing experience.
HyperText Markup Language (HTML)	A language used by web servers to present content to browsers.
HyperText Transfer Protocol (HTTP)	A protocol for communicating on the web.
HyperText Transfer Protocol Secure (HTTPS)	A secure version of HTTP that runs over an encrypted channel (SSL/TLS).
JavaScript	A scripting language commonly integrated into web pages to generate dynamic, interactive content
Mobile Code	Software transmitted from a remote system for execution within a limited execution environment on the local system. Typically, there is no persistent installation and execution begins without the user's consent or even notification. Examples of mobile code technologies include Java applets, Adobe ActionScript, and Microsoft Silverlight. Note that references to mobile code do not refer to JavaScript.
Plug-in	A browser add-on to handle specific types of web content.
Pop-up	A piece of web code that causes a browser to open a window outside the window that is currently in focus.
Port	An application-specific construct that functions as a communications endpoint in a computer's host OS; in a web environment, port 80 is the default port for HTTP communications, although other ports can be used. In a web address, the port follows the domain or sub-domain name (e.g., http://www.cnn.com:80).
Protocol	A system of digital rules for data exchange within or between computers; in a web environment, the typical protocols are HTTP and HTTPS.
Sandbox	A security mechanism for separating running processes, most often used to run untrusted or vulnerable processes by reducing their privileges to such an extent that they should not be able to harm the host system.
Sensitive Data	Sensitive data may include all user or enterprise data or may be specific application data such as data transferred to submit a form or complete a transaction. Sensitive data must minimally include personally identifiable information (PII), credentials, and keys. Sensitive data is expected to be identified in the ST.
Sub-domain	An internet domain which is part of a primary domain, denoted by a prefix before the primary domain (e.g., news.cnn.com).
Tabs	A mechanism that allows a browser to display content from multiple websites in the same window.
Web Browser	An application that retrieves and renders content provided by a web server. The terms web browser, browser, and TOE are interchangeable in this document.

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 Web Browsers

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 Cryptographic Support (FCS)

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed, aside from the fact that the materials for the selections that have been refined out of this SFR are not applicable.

FCS_HTTPS_EXT.1/Client HTTPS Protocol

FCS_HTTPS_EXT.1/Client
There is no change to the Base-PP EAs for this SFR.

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed, aside from the fact that the materials for the selections that have been refined out of this SFR are not applicable.

2.1.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

2.1.1.3 Trusted Path/Channels (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed, aside from the fact that the materials for the selections that have been refined out of this SFR are not applicable.

2.2 TOE SFR Evaluation Activities

2.2.1 User Data Protection (FDP)

FDP_ACF_EXT.1 Local and Session Storage Separation

FDP_ACF_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes how the browser separates local and session storage.

Guidance
The evaluator shall examine the operational guidance to verify that it documents the location on the file system that will be used for local storage and the location used for session storage.

Tests
The evaluator shall obtain or create JavaScript-based scripts that store and retrieve information from local and session storage and shall set up a web server with two or more web pages from different domains using different protocols and ports. The evaluator shall incorporate the scripts into the web pages and shall perform the following tests:

- **Test 1:** The evaluator shall open two or more browser windows/tabs and navigate to the same web page. The evaluator shall verify that the script for accessing session storage that is running in one window/tab cannot access session storage associated with a different window/tab.
- **Test 2:** The evaluator shall open windows/tabs and navigate to different web pages. The evaluator shall verify that a script running in the context of one domain/protocol/port in a browser window/tab cannot access information associated with a different domain/protocol/port in a different window/tab.

FDP_COO_EXT.1 Cookie Blocking

FDP_COO_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes how the browser blocks third-party cookies and when the blocking occurs (e.g., automatically, when blocking is enabled).

Guidance
The evaluator shall examine the operational guidance to verify that it provides a description of the configuration option for blocking of third-party cookies.

Tests
The evaluator shall perform the following tests that may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products:

- **Test 1:** The evaluator shall clear all cookies and then configure the browser so that storage of third-party cookies is allowed. The evaluator shall load a web page that stores a third-party cookie. The evaluator shall navigate to the location where cookies are stored and shall verify that the cookie is present.
- **Test 2:** The evaluator shall clear all cookies and then configure the browser so that storage of third-party cookies is blocked (i.e. not allowed). The evaluator shall load a web page that attempts to store a third-party cookie and shall verify that the cookie was not stored.

FDP_SBX_EXT.1 Sandboxing of Rendering Processes

FDP_SBX_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes how the rendering of HTML and interpretation of JavaScript is performed by the browser in terms of the platform processes that are involved (with "process" being an active entity that executes code). For the processes that render HTML or interpret JavaScript, the evaluator shall examine the TSS to check that it describes how these processes are prevented from accessing the platform file system. The evaluator shall check the TSS to ensure it describes each platform-provided IPC mechanism, and details for each mechanism how the rendering process is unable to use it to communicate with non-browser processes. The evaluator shall also confirm that the TSS describes how IPC and file system access is enabled (if this capability is implemented); for instance, through a more privileged browser process that does not perform web page rendering. The evaluator shall ensure that these descriptions are present for all platforms claimed in the ST.

For each additional mechanism listed in the third bullet of this component by the ST author, the evaluator shall examine the TSS to ensure that:

- the mechanisms are described;
- the description of the mechanisms are sufficiently detailed to determine that it contributes to the principle of least privilege being implemented in the rendering process; and
- appropriate supporting information is provided in the TSS (or pointers to such information are provided) that provides context for understanding the claimed least privilege mechanisms.

Guidance
The evaluator shall examine the operational guidance to determine that it provides a description of the restrictions available on rendering processes. Additionally, if such mechanisms are configurable (for instance, if a user can choose which mechanisms to "turn on"), the evaluator shall examine the operational guidance to

ensure that the method for enabling and disabling the mechanisms are provided, and the consequences of such actions are described.

Tests
The evaluator shall perform the following test on each platform claimed in the ST:

- **Test 1:** The evaluator shall execute a form of mobile code within an HTML page that contains instructions to modify or delete a file from the file system and verify that the file is not modified or deleted.

FDP_SOP_EXT.1 Same Origin Policy

FDP_SOP_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes its implementation of a same origin policy and explains how it complies with RFC 6454. If the browser allows the relaxation of the same origin policy for subdomains in different windows/tabs, the TSS shall describe how these exceptions are implemented.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall obtain or create scripts that can retrieve content from designated locations and shall set up a web server with two or more web pages representing different domains. The evaluator shall incorporate the scripts into the web pages. The evaluator shall associate each page with a different protocol or port and then perform the following tests:

- **Test 1:** The evaluator shall open two or more browser windows/tabs and navigate to a different page on the website in each window/tab. The evaluator shall run the scripts and shall verify that the script that is running in one window/tab cannot access content that was retrieved in a different window/tab.
- **Test 2:** The evaluator shall verify that the scripts can retrieve content from another window/tab at a different subdomain.

FDP_STR_EXT.1 Secure Transmission of Cookie Data

FDP_STR_EXT.1
TSS
The evaluator shall examine the TSS to verify it describes the browser's support for the "secure" attribute of the set-cookie header in accordance with RFC 6265, including the required sending of cookies containing this attribute over HTTPS.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall perform the following tests that may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products:

- **Test 1:** The evaluator shall connect the browser to a cookie-enabled test website implementing HTTPS and have the website present the browser with a "secure" cookie. The evaluator shall examine the browser's cookie cache and verify that that it contains the secure cookie.
- **Test 2:** The evaluator shall reconnect to the cookie-enabled website over an insecure channel and verify that no "secure" cookie is sent.

FDP_TRK_EXT.1 Tracking Information Collection

FDP_TRK_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes the browser's support for tracking information and specifies the tracking information that the browser allows websites to collect about the browser user.

Guidance
The evaluator shall examine the operational guidance to ensure it describes any notifications that the user will receive when tracking information is requested by a website and the options that the user has upon receiving the notification.

Tests
The evaluator shall perform the following tests for each type of tracking information listed in the TSS:

- **Test 1:** The evaluator shall configure a website that requests the tracking information about the user and shall navigate to that website. The evaluator shall verify that the user is notified about the request for tracking information and that, upon consent, the web browser retrieves the tracking information.
- **Test 2:** The evaluator shall verify that the user is notified about the request for tracking information and that, when rejected, the browser does not provide the tracking information.

2.2.2 Security Management (FMT)

FMT_MOF_EXT.1 Management of Functions Behavior

FMT_MOF_EXT.1
TSS
The evaluator shall verify that the TSS describes those management functions which may only be configured by the browser platform administrator and cannot be over-ridden by the user when set according to policy.

Guidance
The evaluator shall examine the operational guidance to verify that it includes instructions for a browser platform administrator to configure the functions listed in FMT_MOF.1.1.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall verify that functions perform as intended by enabling, disabling, and configuring the functions.
- **Test 2:** The evaluator shall create policies that collectively include all management functions controlled by the browser platform administrator and cannot be over-ridden by the user as defined in FMT_MOF.1.1. The evaluator shall apply these policies to the browser, attempt to override each setting as the user, and verify that the browser does not permit it.

2.2.3 Protection of the TSF (FPT)

FPT_AON_EXT.1 Support for Only Trusted Add-ons

FPT_AON_EXT.1
TSS
The evaluator shall verify that the TSS describes whether the browser is capable of loading trusted add-ons.

Guidance
The evaluator shall examine the operational guidance to verify that it includes instructions on loading trusted add-on sources.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall create or obtain an untrusted add-on and attempt to load it. The evaluator shall verify that the untrusted add-on is rejected and cannot be loaded.
- **Test 2:** The evaluator shall create or obtain a trusted add-on and attempt to load it. The evaluator shall verify that the trusted add-on loads.

FPT_DNL_EXT.1 File Downloads

FPT_DNL_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it describes the behavior of the browser when a user initiates the download of a file.

Guidance
The evaluator shall examine the operational guidance to ensure it describes the dialog box that appears when a download is initiated and the implications of the options presented by the dialog box.

Tests
The evaluator shall perform the following test:

- **Test 1:** The evaluator shall navigate to a website that hosts files for download including executables and shall attempt to download and open several of these files. The evaluator shall verify that the browser always presents a dialog box with the option to either download the file to the file system or to discard the file.

FPT_MCD_EXT.1 Mobile Code

FPT_MCD_EXT.1
TSS
The evaluator shall examine the TSS to ensure it lists the types of signed mobile code that the browser supports. The TSS shall describe how the browser handles unsigned mobile code, mobile code from an untrusted source, and mobile code from an unverified source.

Guidance

The following content should be included if:

- provide the user with the option to discard, is selected from FPT_MCD_EXT.1.2

The evaluator shall examine the operational guidance to verify it provides configuration instructions for each of the supported mobile code types. The operational guidance shall also describe the alert that the browser displays to the user when unsigned, untrusted, or unverified mobile code is encountered and the actions the user can take.

Tests
The evaluator shall perform the following test for each mobile code type specified in the TSS:

- **Test 1:** The evaluator shall construct a web page containing correctly signed mobile code and show that it is accepted and executes. The evaluator shall then construct three web pages containing unacceptable mobile code: the first web page contains mobile code that is unsigned; the second web page contains mobile code that is untrusted; the third web page contains mobile code that is unverified. The evaluator shall then attempt to load the mobile code from each of the three web pages, and observe either that the code is rejected or that the user is prompted to accept or reject the code, depending on the selections made in FPT_MCD_EXT.1.2. If the user has the ability to accept or reject the code, the evaluator shall verify that the code is not executed after being rejected.

2.3 Evaluation Activities for Optional SFRs

2.3.1 User Data Protection (FDP)

FDP_PST_EXT.1 Storage of Persistent Information

FDP_PST_EXT.1
TSS
The evaluator shall examine the TSS to verify it describes how the browser operates without storing persistent user data to the file systems.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall perform the following test that may require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products:

- **Test 1:** The evaluator shall operate the browser for a period of time, ensuring that a wide variety of browser functionality has been exercised. The evaluator shall then examine the browser and the underlying platform to ensure that no files have been written to the file system other than the exceptions identified in FDP_PST_EXT.1.1.

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Protection of the TSF (FPT)

FPT_AON_EXT.2 Trusted Installation and Update for Add-ons

FPT_AON_EXT.2
TSS
The evaluator shall examine the TSS to verify that it states that the browser will reject add-ons from untrusted sources.

Guidance
The evaluator shall examine the operational guidance to verify that it includes instructions on how to configure the browser with trusted add-on sources.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall create or obtain an add-on signed by a trusted source and attempt to install it. The evaluator shall verify that the signature on the add-on is valid and that the add-on can be installed.
- **Test 2:** The evaluator shall create or obtain an add-on signed with an invalid certificate and attempt to install it. The evaluator shall verify that the signed add-on is rejected and cannot be installed.
- **Test 3:** The evaluator shall create or obtain an add-on signed by a trusted source, modify the add-on without re-signing it, and attempt to install it. The evaluator shall verify that the signed add-on is rejected and cannot be installed.

2.5 Evaluation Activities for Objective SFRs

2.5.1 Cryptographic Support (FCS)

FCS_STS_EXT.1 Strict Transport Security

FCS_STS_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it documents how the browser supports HSTS.

Guidance
The evaluator shall examine the operational guidance to ensure it contains instructions on how to use HSTS.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall connect to an HSTS-compliant website while running a network protocol analyzer to monitor the traffic. The evaluator shall examine the captured network traffic and verify that a Strict Transport Security header is received and that there is a directive for the max-age of the HSTS relationship.
- **Test 2:** The evaluator shall reconnect to the HSTS website again over HTTP and shall verify that the session is redirected to HTTPS.
- **Test 3:** The evaluator shall reconnect to the HSTS website after the max-age has expired, and verify that the website and browser reestablish an HSTS relationship.
- **Test 4:** The evaluator shall update the website HSTS information, and verify that when the browser reconnects to the website, that information is updated by the browser.

2.5.2 Protection of the TSF (FPT)

FPT_INT_EXT.1 Interactions with Application Reputation Services

FPT_INT_EXT.1
TSS
The evaluator shall examine the TSS to ensure it describes the browser's use of application reputation services in detecting malicious applications.

Guidance
The evaluator shall examine the operational guidance to ensure it describes the browser's support for use of an application reputation service, including which services the browser supports by default (if any) and whether additional services can be configured. The operational guidance shall include steps for how to configure the application reputation service.

Tests
The evaluator shall perform the following test:

- **Test 1:** The evaluator shall configure the browser to enable the use of one or more application reputation services per the operational guidance. The evaluator shall initiate a connection with a website that attempts to download an application to the browser while sniffing the network traffic using a network protocol analyzer. The evaluator shall inspect the captured network traffic and shall verify that the browser initiates a connection to the configured application reputation service(s) before initiating the download.

FPT_INT_EXT.2 Interactions with URL Reputation Services

FPT_INT_EXT.2
TSS
The evaluator shall examine the TSS to ensure it describes the browser's use of a URL reputation service in detecting malicious websites.

Guidance
The evaluator shall examine the operational guidance to ensure it describes the browser's support for use of URL reputation services, including which services the browser supports by default (if any) and whether additional services can be configured. The operational guidance shall include steps for how to configure the URL reputation service.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall configure the browser to enable the use of one or more URL reputation services per the operational guidance. The evaluator shall initiate a connection with a known good website while sniffing the network traffic using a network protocol analyzer. The evaluator shall inspect the captured network traffic and shall verify that the browser initiates a connection to the configured URL reputation service(s).
- **Test 2:** The evaluator shall configure the browser to enable the use of one or more URL reputation services per the operational guidance. The evaluator shall initiate a connection with a known malicious website that is identified by one or more of the URL reputation services while sniffing the network traffic using a network protocol analyzer. The evaluator shall verify that a warning appears alerting that the website is known to be malicious and the browser is not allowed to connect. The evaluator shall inspect

the captured network traffic and shall verify that the browser initiates a connection to the configured URL reputation service(s) and retrieved an updated list of malicious URLs with the tested website being on the list.

3 Evaluation Activities for SARs

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

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.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1r5, CCMB-2017-04-004, April 2017
[App PP]	Protection Profile for Application Software, Version 1.3, March 1, 2019