PP-Module for Web Browsers

Version: 1.0
2021-06-18
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2021-06-18	Initial release as PP-Module

Contents

1 Introduction
1.1 Overview
1.2 Terms
1.2.1 Common Criteria Terms
1.2.2 Technical Terms
1.3 Compliant Targets of Evaluation
1.3.1 TOE Boundary
1.4 Use Cases
2 Conformance Claims
3 Security Problem Description
3.1 Threats
3.2 Assumptions
3.3 Organizational Security Policies
4 Security Objectives
4.1 Security Objectives for the TOE
4.2 Security Objectives for the Operational Environment
4.3 Security Objectives Rationale
5 Security Requirements
5.1 Application Software PP Security Functional Requirements Direction
5.1.1 Modified SFRs
5.1.1.1 Cryptographic Support (FCS)
5.1.1.2 Identification and Authentication (FIA)
5.1.1.3 Trusted Path/Channels (FTP)
5.2 TOE Security Functional Requirements
5.2.1 User Data Protection (FDP)
5.2.2 Security Management (FMT)
5.2.3 Protection of the TSF (FPT)
5.3 TOE Security Functional Requirements Rationale
6 Consistency Rationale
6.1 Protection Profile for Application Software
6.1.1 Consistency of TOE Type
6.1.2 Consistency of Security Problem Definition
6.1.3 Consistency of Objectives
6.1.4 Consistency of Requirements
Appendix A - Optional SFRs
A.1 Strictly Optional Requirements
A.1.1 User Data Protection (FDP)
A.2 Objective Requirements
A.2.1 Cryptographic Support (FCS)
A.2.2 Protection of the TSF (FPT)
A.3 Implementation-Based Requirements
Appendix B - Selection-Based Requirements
B.1 Protection of the TSF (FPT)
Appendix C - Extended Component Definitions
C.1 Extended Components Table
C.2 Extended Component Definitions
C.2.1 FDP_ACF_EXT Access Control Functions
C.2.2 FDP_COO_EXT Cookie Blocking
C.2.3 FDP_SBX_EXT Sandboxing
C.2.4 FDP_SOP_EXT Same Origin Policy
C.2.5 FDP_STR_EXT Secure Transmission of Cookie Data
C.2.6 FDP_TRK_EXT Tracking Information Collection
C.2.7 FMT_MOF_EXT Management of Functions Behavior
C.2.8 FPT_AON_EXT Add-Ons
C.2.9 FPT_DNL_EXT File Downloads
C.2.10 FPT_MCD_EXT Mobile Code
C.2.11 FDP_PST_EXT Storage of Persistent Information
C.2.12 FCS_STS_EXT Strict Transport Security
C.2.13 FPT_INT_EXT Reputation Service Interaction
Appendix D - Entropy Documentation and Assessment
Appendix E - Acronyms
Appendix F - Bibliography

1 Introduction

1.1 Overview

The scope of the Web Browser PP-Module is to describe the security functionality of web browser applications in terms of [CC] and to define functional and assurance requirements for the product-specific capabilities of web browser applications. Web browsers are client applications that retrieve and render content provided by web servers, primarily using the hypertext transfer protocol (HTTP) or HTTP Secure (HTTPS). This PP-Module is intended for use with the following Base-PP:

- Protection Profile for Application Software, Version 1.3

This Base-PP is valid because web browsers are a specific type of software application.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 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.
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.
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 Protection Profiles.
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.
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.

Target of Evaluation (TOE)	The product under evaluation.

1.2.2 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 Forgery (CSRF)	A vulnerability where an attacker gets a target user to execute a script with that user's 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.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this PP-Module is a web browser application running on a desktop or mobile operating system.

Web browsers are client applications that retrieve and render content provided by web servers, primarily using the hypertext transfer protocol (HTTP) or HTTP Secure (HTTPS). Browsers have grown in complexity over the years, starting as tools used to display simple, unchanging websites and becoming sophisticated execution environments for web content. The use of browsers to administer accounts, servers, or embedded systems remotely requires them to handle sensitive information securely. Innovations such as tabs, extensions, and HTML5 have not only increased browser functionality, but also introduced new security concerns. Being the principal method for accessing the internet, and due to their complexity and the information that they process, browsers are a natural target for attackers. As a result, it is paramount that the security of web browsers be improved to reduce the risk to client machines and enterprise networks.

This PP-Module along with the Protection Profile for Application Software [App PP] provide a baseline set of Security Functional Requirements (SFRs) for web browsers running on any operating system regardless of the composition of the underlying platform. The requirements are intended to improve the security of browsers by encouraging the use of operating system security services and requiring the use of sandboxing technologies and environmental mitigations provided by the underlying platform. Additionally, these requirements define security functionality that browsers must provide.

The terms web browser, browser, and TOE are interchangeable in this document.

1.3.1 TOE Boundary

The physical boundary of the web browser is a software application running on a general-purpose operating system. The TOE boundary may include third-party add-ons, but these are non-interfering with respect to security; add-ons provide features that are outside the TOE's logical boundary but must be implemented in such a manner that their inclusion does not compromise the security of the TSF.

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problems in the use cases below. These use cases are intentionally very broad, as web browsers can be used to perform many tasks.

[USE CASE 1] Surfing the Web

Browsers are used to retrieve, display, and render content from the web, such as websites, streaming media, images, and specialized formats (e.g., Java, PDF). They can also be used to write content to websites (web 2.0 – e.g., Facebook). Web surfing can be done over the internet or within an intranet.

[USE CASE 2] Remote Administration Client

Browsers are used to provide remote administration interfaces for systems such as servers, network devices, and embedded systems, to include supervisory control and data acquisition (SCADA) systems, smart TVs, and thermostats. As opposed to surfing the web, where the browser may be interacting with untrusted content, the browser, acting as a Remote Administration Client, is connecting to a server that the user trusts.

[USE CASE 3] Content Creation

Browsers are used to create content via an increasing number of Software as a Service (SaaS) offerings, including Microsoft Office 365, Google Drive, and Adobe Creative Cloud, where user data and records are stored online.

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

No additional PPs or PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module aside from the Base-PP.

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (extended) of Common Criteria Version 3.1, Release 5 [CC].

Package Claims

This PP-Module is TLS Pacakge conformant.

3 Security Problem Description

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

This PP-Module does not repeat the threats, assumptions, and organizational security policies identified in the App PP, though they all apply given the conformance and hence dependence of this PP-Module on it. Together the threats, assumptions and organizational security policies of the App PP and those defined in this PP-Module describe those addressed by a web browser as the Target of Evaluation.

Notably, browsers are particularly at risk from the T.NETWORK_ATTACK threat identified in the App PP. Attackers can use phishing or another social engineering technique to persuade a user to visit a malicious site. Users may also unintentionally visit malicious sites in the course of web browsing. Such sites then present malicious content to the user's browser to exploit it and perform installation of malware, often with no indication to the user.

3.1 Threats

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

T.FLAWED_ADDON
Web browser functionality can be extended through the integration of third-party utilities and tools. Malicious or vulnerable add-ons could result in attacks against the system. Such attacks can allow unauthorized access to sensitive information in the browser, unauthorized access to the platform's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.

T.NETWORK_ATTACK
See App PP, Section 3.1.

T.NETWORK_EAVESDROP
See App PP, Section 3.1.

T.PHYSICAL_ACCESS
See App PP, Section 3.1.

T.SAME_ORIGIN_VIOLATION
Violating the same-origin policy is a specialized type of network attack (covered generally as T.NETWORK_ATTACK in the App PP) which involves web content violating access control policies enforced by a web browser to separate the content of different web domains. It is specifically identified as a threat to web browsers, since they implement the access control policies that are violated in these attacks.

Attacks which involve same origin violations include:

- Insufficient protection of session tokens can lead to session hijacking, where a token is captured and reused in order to gain the privileges of the user who initiated the session.
- XSS and CSRF attacks are methods used to compromise user credentials (usually by stealing the user's session token) to a website. These attacks are more likely a result of server security problems, but some browsers incorporate technologies that try to detect the attacks.
- Inadequate sandboxing of browser windows/tabs or a faulty cross domain communications model can lead to leakage of content from one domain in one window/tab to a different domain in a different window/tab. Such attacks leverage the ability of browsers to display content from multiple domains simultaneously.

3.2 Assumptions

This document does not define any additional assumptions.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed base PP.

This document does not define any additional OSPs.

4 Security Objectives

This PP-Module adds SFRs to objectives identified in the Base-PP and describes additional objectives specific to this PP-Module.

4.1 Security Objectives for the TOE

O.INTEGRITY
This objective is defined in the Base-PP. This PP-Module maps additional SFRs to it to address the integrity protection mechanisms that are specific to web browser applications.

O.MANAGEMENT
This objective is defined in the Base-PP. This PP-Module maps additional SFRs to it to address the management functionality that is specific to web browser applications.

O.PROTECTED_STORAGE
This objective is defined in the Base-PP. This PP-Module maps additional SFRs to it to address the data at rest protection functionality that is specific to web browser applications.

O.PROTECTED_COMMS
This objective is defined in the Base-PP. This PP-Module maps additional SFRs to it to address the data in transit protection functionality that is specific to web browser applications.

O.DOMAIN_ISOLATION
To address the network attack associated with content leakage between different web domains, the browser must ensure that content originating from different domains (e.g., in a tab or iFrame) is properly isolated.

O.ADDON_INTEGRITY
To address issues associated with malicious or flawed add-ons, conformant browsers implement mechanisms to ensure their integrity. This includes verification and validation at installation time and update.

4.2 Security Objectives for the Operational Environment

This PP-Module does not define any objectives for the Operational Environment.

No environmental security objectives have been identified that are specific to web browsers. However, any environmental security objectives defined in the Base-PP will also apply to the portion of the TOE that implements web browser functionality.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.FLAWED_ADDON	O.ADDON_INTEGRITY	The threat T.FLAWED_ADDON is countered by O.ADDON_INTEGRITY, which ensures that a conformant TOE either does not support add-ons at all (in which case there is no possibility of it executing a flawed add-on) or that it supports only add-ons that can prove their integrity.
T.NETWORK_ATTACK	O.INTEGRITY	The threat T.NETWORK_ATTACK is countered by O.INTEGRITY as this provides for the ability of the TOE to resist unauthorized modification via a network vector.
	O.MANAGEMENT	The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT as this provides for the ability to configure the application to defend against network attack.
	O.PROTECTED_COMMS	The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS as this provides for integrity of transmitted data.
T.NETWORK_EAVESDROP	O.MANAGEMENT	The threat T.NETWORK_EAVESDROP is countered by O.MANAGEMENT as this provides for the ability to configure the application to protect the confidentiality of its

		transmitted data.
	O.PROTECTED_COMMS	The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS as this provides for confidentiality of transmitted data.
T.PHYSICAL_ACCESS	O.PROTECTED_STORAGE	The threat T.PHYSICAL_ACCESS is countered by O.PROTECTED_STORAGE, which protects against unauthorized attempts to access physical storage used by the TOE.
T.SAME_ORIGIN_VIOLATION	O.DOMAIN_ISOLATION	The threat T.SAME_ORIGIN_VIOLATION is countered by O.DOMAIN_ISOLATION, which ensures that a conformant TOE will prevent leakage of content between multiple windows/tabs being rendered by the same application.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, 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: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Application Software PP Security Functional Requirements Direction

In a PP-Configuration that includes Application Software PP, the TOE is expected to rely on some of the security functions implemented by the as a whole and evaluated against the Application Software PP. The following sections describe any modifications that the ST author must make to the SFRs defined in the Application Software PP in addition to what is mandated by Section 5.2 TOE Security Functional Requirements.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the Application Software PP and relevant to the secure operation of the TOE.

5.1.1.1 Cryptographic Support (FCS)

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [**selection**:

- *invoke platform-provided functionality for asymmetric key generation,*
- *implement asymmetric key generation*

].

Application Note: This SFR is modified from its Base-PP definition to remove the selection for the TOE not requiring asymmetric key generation.

Evaluation Activities

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.1.1/Client

This SFR is selection-based in the App PP. When the TOE conforms to this PP-Module, it is mandatory because of the modifications that this PP-Module makes to FTP_DIT_EXT.1.

Evaluation Activities

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.1.1

The application shall [**selection**:

- *invoke platform-provided DRBG functionality,*
- *implement DRBG functionality*

] for its cryptographic operations.

Application Note: This SFR is modified from its Base-PP definition to remove

the selection for the TOE using no DRBG functionality.

Evaluation Activities

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.

5.1.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1

This SFR is selection-based in the App PP. When the TOE conforms to this PP-Module, it is mandatory because of the modifications that this PP-Module makes to FTP_DIT_EXT.1.

Evaluation Activities

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.2.1

This SFR is selection-based in the App PP. When the TOE conforms to this PP-Module, it is mandatory because of the modifications that this PP-Module makes to FTP_DIT_EXT.1.

Evaluation Activities

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

5.1.1.3 Trusted Path/Channels (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall

- *encrypt all transmitted [sensitive data] with [HTTPS in accordance with FCS_HTTPS_EXT.1**/Client**, TLS as defined in the TLS Package, DTLS as defined in the TLS Package]*

between itself and another trusted IT product.

Application Note: This SFR is modified from its definition in the App PP to require that the TOE supports TLS and DTLS and that its use of these protocols is only limited to sensitive data. A conformant TOE must support the use of both TLS and HTTPS for secure web browsing but is permitted to interact with non-sensitive content over an untrusted channel.

Either the TOE or its platform is permitted to implement TLS and DTLS. If the TOE implements these protocols, FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_TLS_EXT.1, FCS_TLSC_EXT.1, and FCS_TLSC_EXT.2 from the TLS package must be claimed at minimum because a web browser is required to support mutually-authenticated TLS and DTLS.

Evaluation Activities

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.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 User Data Protection (FDP)

FDP_ACF_EXT.1 Local and Session Storage Separation

FDP_ACF_EXT.1.1

The TSF shall separate local (permanent) and session (ephemeral) storage based on domain, protocol, and port:

- Session storage shall be accessible only from the originating window/tab;
- Local storage shall only be accessible from windows/tabs running the same web application.

Application Note: The separation of local and session storage is described in World Wide Web Consortium (W3C) Proposed Recommendation: "Web Storage."

Evaluation Activities

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.1.1

The TSF shall provide the capability to block the storage of third-party cookies by websites.

Evaluation Activities

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.1.1

The TSF shall ensure that web page rendering is performed in a process that is

restricted in the following manner:

- The rendering process can only directly access the area of the file system dedicated to the browser.
- The rendering process can only directly invoke inter-process communication mechanisms with its own browser processes.
- The rendering process has reduced privilege with respect to other browser processes [**selection**: *[**assignment**: other methods by which the principle of least privilege is implemented for rendering processes], in no other ways*].

Application Note: Web browsers implement a variety of methods to ensure that the process that renders HTML and interprets JavaScript operates in a constrained environment in order to reduce the risk that the rendering process can be corrupted by the HTML or JavaScript it is processing. This component requires the browser to lower the privileges of rendering processes by ensuring that it cannot directly access the file system of the host, and that it cannot use inter-process communication (IPC) mechanisms provided by the host to communicate with non-browser processes on the host. Typically, if a rendering process needs to access a file or communicate with a non-browser process, it must request such access through the TSF (which is allowed by the requirement).

In addition to the two required measures, other measures can be implemented depending on the browser and the host platform. These may involve such actions as changing the owner of the rendering process to a low-privileged account or dropping platform-defined privileges in the rendering process. The ST author fills in the additional measures implemented by the browser.

Evaluation Activities

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.1.1

The TSF shall only permit scripts contained in one web page to access data in a second web page if both pages are from the same origin.

FDP_SOP_EXT.1.2

The TSF shall enforce the same origin policy for all domains.

Application Note: The Same Origin Policy concept is described in RFC 6454, "The Web Origin Concept." Origin is defined as the combination of domain, protocol, and port. Two URIs sharing the same domain, protocol, and port are

considered to have the same origin.

Evaluation Activities

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.1.1

The TSF shall ensure that cookies containing the 'secure' attribute in the set-cookie header are sent over HTTPS.

Application Note: The set-cookie header functionality is described in RFC 6265, "HTTP State Management Mechanism."

Evaluation Activities

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.1.1

The TSF shall provide notification to the user when tracking information for [**selection**:

- *geolocation*,
- *browser history*,
- *browser preferences*,
- *browser statistics*

] is requested by a website.

Evaluation Activities

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.*

5.2.2 Security Management (FMT)

FMT_MOF_EXT.1 Management of Functions Behavior

FMT_MOF_EXT.1.1

The TSF shall be capable of performing the following management functions, controlled by the administrator or user as shown:

- M = Mandatory
- O = Optional

#	Management Function	Administrator	User
1	Enable/disable storage of third-party cookies	O	M
2	Enable/disable use of OCSP for obtaining the revocation status of X.509 certificates	O	O
3	Configure inclusion of user-agent information in HTTP headers	O	O
4	Enable/disable ability for websites to collect tracking information about the user through [**selection**: *zombie cookies, add-on based tracking (e.g. Flash cookies), browsing history, [**assignment**: other tracking mechanisms]*]	O	O
5	Enable/disable deletion of stored browsing data (cache, web form information)	O	M
6	Enable/disable storage of sensitive information (e.g., auto-fill, auto-complete) in persistent storage	O	O
7	Configure size of cookie cache	O	O
8	Configure size of cache	O	O
9	Enable/disable interaction with Graphic Processing Units (GPUs)	O	O
10	Configure the ability to advance to a website with an invalid or unvalidated X.509 certificate	O	O
11	Enable/disable establishment of a trusted channel if the browser cannot establish a connection to determine the validity of a certificate	O	O
12	Configure the use of an application reputation service to detect malicious applications prior to download	O	O
13	Configure the use of a URL reputation service to detect sites that contain malware or phishing content	O	O
14	Enable/disable automatic installation of software updates and patches	O	O
15	Enable/disable ability for websites to register protocol handlers	O	O

16	Enable/disable display notification when unsigned, untrusted, or unverified mobile code is encountered	O	O
17	Enable/disable user's ability to select default actions upon download of a file (e.g., always open, or always save, a downloaded file)	O	O
18	Enable/disable launching of downloaded files outside the browser	O	O
19	Enable/disable JavaScript	O	O
20	Enable/disable [**selection**: *ActiveX, Flash, Java, [**assignment**: other mobile code types supported by the browser]*] mobile code	O	O
21	Enable/disable support for add-ons	O	O
22	Enable/disable individual add-ons	O	O
23	Enable/disable HSTS mode	O	O

Application Note: For these management functions, the term "Administrator" refers to the administrator of a non-mobile device or the device owner of a mobile device. The intent of this requirement is to allow the user and administrator of the platform to configure the browser with configuration policies. If the administrator has not set a policy for a particular function, the user may still perform that function. Enforcement of the policy is done by the browser itself, or the browser and its platform in coordination with each other.

Disabling OCSP is only be permitted if "CRL" was selected in FIA_X509_EXT.1.1 (in App PP).

Evaluation Activities

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.*

5.2.3 Protection of the TSF (FPT)

FPT_AON_EXT.1 Support for Only Trusted Add-ons

FPT_AON_EXT.1.1

The TSF shall include the capability to load [**selection**: *trusted add-ons, no add-ons*].

Application Note: If "trusted add-ons" is selected in FPT_AON_EXT.1.1, the TOE must also claim the selection-based SFR FPT_AON_EXT.2.

If the browser does not include support for installing only trusted add-ons, this requirement can be met by demonstrating the ability to disable all support for add-ons as specified in FMT_MOF_EXT.1.

Evaluation Activities

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.1.1

The TSF shall prevent downloaded content from launching automatically.

FPT_DNL_EXT.1.2

The TSF shall present the user with the option to either save or discard downloaded files.

Application Note: This requirement ensures that if the user intentionally (via clicking on a link) or unintentionally initiates the download of a file, the browser will intervene by, for example, opening a dialog box that presents the user with the option to either save the file to the file system or not download the file.

In this context, an executable is a file containing code for a software program that is invoked independent of and outside the context of the browser. It does not include mobile code, scripts, or add-ons.

Evaluation Activities

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.1.1

The TSF shall support the capability to execute [**selection**:

- *signed [**selection**:*
  - *ActiveX,*
  - *Flash,*
  - *Java,*
  - *ActionScript,*
  - *[**assignment**: other mobile code types supported by the browser]*

  ],
- *no*

] mobile code.

FPT_MCD_EXT.1.2

The TSF shall [**selection**: *automatically discard*, *provide the user with the option to discard*] unsigned, untrusted, or unverified [**selection**:

- *ActiveX,*
- *Flash,*
- *Java,*
- *ActionScript,*
- *[**assignment**: other mobile code types supported by the browser]*

] mobile code without executing it.

Application Note: The ST author must specify all mobile code types for which the browser provides this support.

An authorized signer may directly sign the code itself, or the code may be delivered over an authenticated HTTPS connection with an authorized entity.

Evaluation Activities

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
If "proivde the user with the option discard" is selected in 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.*

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 2: SFR Rationale

Objective	Addressed by	Rationale
O.INTEGRITY	FPT_DNL_EXT.1, FPT_MCD_EXT.1, FPT_INT_EXT.1 (objective)	FDP_DNL_EXT.1 supports the objective by preventing the automatic execution of downloaded files which could otherwise cause integrity violations to the TOE itself or to its platform. FDP_MCD_EXT.1 supports the objective by preventing the automatic execution of mobile code which could otherwise cause integrity violations to the TOE itself or to its platform. FPT_INT_EXT.1 supports the objective by optionally requiring the TSF to implement a reputation service to prevent the acquisition of potentially malicious applications.
O.MANAGEMENT	FDP_TRK_EXT.1, FMT_MOF_EXT.1	FDP_TRK_EXT.1 supports the objective by notifying the user when various data is being tracked to allow for control of the disclosure of configuration information. FMT_MOF_EXT.1 supports the objective by defining the management functionality that is specific to web browser applications.
O.PROTECTED_STORAGE	FDP_COO_EXT.1, FDP_PST_EXT.1 (optional), FPT_INT_EXT.1 (objective)	FDP_COO_EXT.1 supports the objective by defining a mechanism to prevent

		untrusted data from being loaded into protected storage. FDP_PST_EXT.1 supports the objective by optionally defining the minimum set of persistent data that the TSF is required to store. FPT_INT_EXT.1 supports the objective by optionally requiring the TSF to implement a mechanism to protect against downloading known malicious applications that may adversely affect data stored at rest.
O.PROTECTED_COMMS	FCS_CKM_EXT.1 (modified from Base-PP), FCS_HTTPS_EXT.1/Client (from Base-PP), FCS_RBG_EXT.1 (modified from Base-PP), FIA_X509_EXT.1 (from Base-PP), FIA_X509_EXT.2 (from Base-PP), FTP_DIT_EXT.1 (modified from Base-PP), FDP_STR_EXT.1, FCS_STS_EXT.1 (objective), FPT_INT_EXT.2 (objective)	FCS_CKM_EXT.1 supports the objective by requiring that the TSF provide or invoke a cryptographic function for asymmetric key generation. FCS_HTTPS_EXT.1/Client supports the objective by defining the TSF's implementation of HTTPS. FCS_RBG_EXT.1 supports the objective by requiring that the TSF provide or invoke a DRBG for secure key generation. FIA_X509_EXT.1 supports the objective by requiring the TSF to implement or invoke an X.509 certificate validation service. FIA_X509_EXT.2 supports the objective by defining the TOE's use of X.509 certificates and what behavior the TOE takes when the revocation status of a certificate cannot be determined. FTP_DIT_EXT.1 supports the objective by specifying the trusted communications channels used by the TOE to protect data in transit. FDP_STR_EXT.1 supports the objective by requiring the use of HTTPS for certain types of data transfer. FCS_STS_EXT.1 supports the objective by optionally requiring the TSF to implement HSTS for secure data transmission. FPT_INT_EXT.2 supports the objective by optionally requiring the TSF to implement a URL reputation service that can block communications with malicious entities.
O.DOMAIN_ISOLATION	FDP_ACF_EXT.1, FDP_SBX_EXT.1, FDP_SOP_EXT.1	FDP_ACF_EXT.1 supports the objective by isolating local and session storage to its origin point. FDP_SBX_EXT.1 supports the objective by ensuring that rendering of content is isolated to its origin point. FDP_SOP_EXT.1 supports the objective by enforcing the concept of a same origin policy

		to prevent web content with different origins from interacting with one another.
O.ADDON_INTEGRITY	FPT_AON_EXT.1, FPT_AON_EXT.2 (selection-based)	FPT_AON_EXT.1 supports the objective by specifying whether or not the TSF has the ability to load add-ons. FPT_AON_EXT.2 supports the objective by defining a cryptographic method for the TSF to validate the integrity of add-ons if the TOE supports their use.

6 Consistency Rationale

6.1 Protection Profile for Application Software

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is simply extended to include the web browser functionality that is built into the application so that additional security functionality is claimed within the scope of the TOE.

6.1.2 Consistency of Security Problem Definition

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.FLAWED_ADDON	The threat of a user installing a flawed add-on is consistent with the T.LOCAL_ATTACK threat from the Base-PP. A flawed add-on, whether crafted deliberately or unintentionally, could cause the product to operate in a manner where it or its platform can be compromised.
T.NETWORK_ATTACK	This threat comes directly from the Base-PP.
T.NETWORK_EAVESDROP	This threat comes directly from the Base-PP.
T.PHYSICAL_ACCESS	This threat comes directly from the Base-PP.
T.SAME_ORIGIN_VIOLATION	This threat extends the security problem definition of the Base-PP by defining a potential vulnerability that specifically applies to the content that is handled by web browsers.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the Application Software PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.INTEGRITY	This objective is an enhancement to the O.INTEGRITY objective defined in the Base-PP, specifically in regards to the integrity protection mechanisms that apply to web browsers.
O.MANAGEMENT	This objective is an enhancement to the O.MANAGEMENT objective defined in the Base-PP, specifically in regards to the secure administration of functions that are specific to web browser applications.
O.PROTECTED_STORAGE	This objective is an enhancement to the O.PROTECTED_STORAGE objective defined in the Base-PP, specifically in regards to the data at rest that applies to web browser applications.
O.PROTECTED_COMMS	This objective is an enhancement to the O.PROTECTED_COMMS objective defined in the Base-PP, specifically in regards to the data in transit that applies to web browser applications.
O.DOMAIN_ISOLATION	This objective applies to functionality that is specific to web browser applications and is therefore beyond the original scope of the Base-PP.
O.ADDON_INTEGRITY	This objective is an enhancement to the O.INTEGRITY objective defined in the Base-PP. Where O.INTEGRITY is concerned with the integrity of the TOE application, O.ADDON_INTEGRITY is concerned with the integrity of third-party add-ons that can be loaded into the TOE.

This PP-Module does not define any objectives for the TOE's operational environment.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the Application Software PP that are needed to support Web Browsers functionality. This is considered to be consistent because the functionality provided by the Application Software PP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the Application Software PP that are used entirely to provide functionality for Web Browsers. The rationale for why this does not conflict with the claims defined by the Application Software PP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
FCS_CKM_EXT.1	This SFR is changed from its definition in the App PP to remove one of the

	available selection options because it will never apply in the case where the TOE conforms to this PP-Module.
FCS_HTTPS_EXT.1/Client	This SFR is unchanged from its definition in the App PP; the SFR is recategorized from selection-based to mandatory when the TOE conforms to this PP-Module.
FCS_RBG_EXT.1	This SFR is changed from its definition in the App PP to remove one of the available selection options because it will never apply in the case where the TOE conforms to this PP-Module.
FIA_X509_EXT.1	This SFR is unchanged from its definition in the App PP; the SFR is recategorized from selection-based to mandatory when the TOE conforms to this PP-Module.
FIA_X509_EXT.2	This SFR is unchanged from its definition in the App PP; the SFR is recategorized from selection-based to mandatory when the TOE conforms to this PP-Module.
FTP_DIT_EXT.1	This SFR is changed from its definition in the App PP to mandate the protection of sensitive data using only specified protocols.
Mandatory SFRs	
FDP_ACF_EXT.1	This SFR defines domain separation of web content when a web browser is simultaneously accessing content from multiple sources. It does not impact the App PP functionality.
FDP_COO_EXT.1	This SFR defines behavior for handling cookies, which are data specific to web browser applications. It does not impact the App PP functionality.
FDP_SBX_EXT.1	This SFR defines behavior for rendering of web pages, which is by definition functionality that is associated with web browser applications. It does not impact the App PP functionality.
FDP_SOP_EXT.1	This SFR defines behavior for script execution on web pages, which is by definition functionality that is associated with web browser applications. It does not impact the App PP functionality.
FDP_STR_EXT.1	This SFR defines behavior for handling cookies, which are data specific to web browser applications. It does not impact the App PP functionality.
FDP_TRK_EXT.1	This SFR defines behavior for handling tracking information that is specific to web browser applications. It does not impact the App PP functionality.
FMT_MOF_EXT.1	This SFR defines a specific set of management functions for a web browser. It does not impact the App PP functionality.
FPT_AON_EXT.1	This SFR defines what types of plugins a web browser may use. It does not impact the App PP functionality.
FPT_DNL_EXT.1	This SFR defines behavior for handling file data that can be downloaded by a web browser. It does not impact the App PP functionality.
FPT_MCD_EXT.1	This SFR defines behavior for mobile code that is rendered by a web browser. It does not impact the App PP functionality.
Optional SFRs	
FDP_PST_EXT.1	This SFR defines the persistent information that must be stored for web browser functionality to work as intended. It does not impact functionality described by the App PP.
Selection-based SFRs	
FPT_AON_EXT.2	This SFR defines how web browsers verify add-ons. It does not impact functionality described by the App PP.
Objective SFRs	
FCS_STS_EXT.1	This SFR defines behavior for implementation of HSTS, which is a communications mechanism specific to web content. It does not impact the App PP functionality.
FPT_INT_EXT.1	This SFR defines behavior interaction with a reputation service for file data that the TOE can be used to download. It does not impact the App PP functionality.
FPT_INT_EXT.2	This SFR defines behavior interaction with a reputation service for web content that the TOE can be used to interact with. It does not impact the App PP functionality.
Implementation-Dependent SFRs	

This PP-Module does not define any Implementation-Dependent requirements.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 User Data Protection (FDP)

FDP_PST_EXT.1 Storage of Persistent Information

FDP_PST_EXT.1.1

The TSF shall provide the capability to operate without storing persistent data to the file system with the following exceptions: [**selection**: *credential information*, *administrator provided configuration information*, *certificate revocation information*, *no exceptions*].

Application Note: Any data that persists after the browser closes, including temporary files, is considered to be persistent data.

Evaluation Activities

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.*

A.2 Objective Requirements

A.2.1 Cryptographic Support (FCS)

FCS_STS_EXT.1 Strict Transport Security

FCS_STS_EXT.1.1

The TSF shall implement HTTP Strict-Transport-Security according to RFC 6797.

FCS_STS_EXT.1.2

The TSF shall retain persistent data signaling HSTS enablement for the time span declared by the website in a max-age directive.

FCS_STS_EXT.1.3

The TSF shall cache the "freshest" Strict Security policy information.

Application Note: Freshness refers to the length of time between generation by the origin server and the expiration time when the origin server specifies that a stored response can no longer be used by a cache without further validation (RFCs 6797 and 7234). If a browser receives the HSTS header from a website, all future HTTP sessions between the browser and the domain or superdomain of that website must occur over TLS 1.2 (RFC 5246) or greater by using HTTPS (RFC 2818) negotiating the strongest cipher possible.

Evaluation Activities

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.*

A.2.2 Protection of the TSF (FPT)

FPT_INT_EXT.1 Interactions with Application Reputation Services

FPT_INT_EXT.1.1

The TSF shall use an application reputation service to prevent downloading of malicious applications.

Application Note: An application reputation service is an online service that identifies malicious applications; it is used to detect such applications prior to downloading them. Using a reputation service would require configuration of the trusted service to be used. The quality of the reputation service may fall outside of the scope of the evaluation.

Evaluation Activities

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.2.1

The TSF shall use a URL reputation service to prevent connections with malicious websites.

Application Note: A URL reputation service is an online service that identifies websites with malicious or phishing content applications; it is used to detect such websites prior to allowing users to access them. The goal of this requirement is to ensure that the browser is prevented from establishing connections with known-bad sources of malware on the internet. The specifics of the sequence of actions taken before a block decision is made may depend upon the specific implementation of the browser. For example, some browsers might implement the check for malicious content by checking against the list of bad URLs provided by the URL reputation service in real time; others may download updated lists of bad URLs at browser startup, updating the list periodically from the URL reputation service(s) until the browser is terminated. Ultimately, the result should be that the browser blocks the connection to the bad URL.

Evaluation Activities

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.*

A.3 Implementation-Based Requirements

This PP-Module does not define any Implementation-Based SFRs.

Appendix B - Selection-Based Requirements

B.1 Protection of the TSF (FPT)

FPT_AON_EXT.2 Trusted Installation and Update for Add-ons

The inclusion of this selection-based component depends upon a selection in FPT_AON_EXT.1.1.

FPT_AON_EXT.2.1

The TSF shall [**selection**: *provide the ability*, *leverage the platform*] to provide a means to cryptographically verify add-ons using a digital signature mechanism and [**selection**: *published hash*, *no other functions*] prior to installation and update.

FPT_AON_EXT.2.2

The TSF shall [**selection**: *provide the ability*, *leverage the platform*] to query the current version of the add-on.

FPT_AON_EXT.2.3

The TSF shall prevent the automatic installation of add-ons.

Application Note: This selection-based SFR is claimed when "trusted add-ons" is selected in FPT_AON_EXT.1.1.

Evaluation Activities

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.*

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 3: Extended Component Definitions

Functional Class	Functional Components
User Data Protection (FDP)	FDP_ACF_EXT Access Control Functions FDP_COO_EXT Cookie Blocking FDP_PST_EXT Storage of Persistent Information FDP_SBX_EXT Sandboxing FDP_SOP_EXT Same Origin Policy FDP_STR_EXT Secure Transmission of Cookie Data FDP_TRK_EXT Tracking Information Collection
Security Management (FMT)	FMT_MOF_EXT Management of Functions Behavior
Protection of the TSF (FPT)	FPT_AON_EXT Add-Ons FPT_DNL_EXT File Downloads FPT_INT_EXT Reputation Service Interaction FPT_MCD_EXT Mobile Code
Cryptographic Support (FCS)	FCS_STS_EXT Strict Transport Security

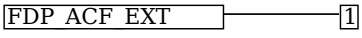
C.2 Extended Component Definitions

C.2.1 FDP_ACF_EXT Access Control Functions

Family Behavior

Components in this family define requirements for data access control beyond those which are specified in the Part 2 family FDP_ACF.

Component Leveling



FDP_ACF_EXT.1, Local and Session Storage Separation, requires the TSF to enforce data protection mechanisms such that user data is only accessible from its originator.

Management: FDP_ACF_EXT.1

No specific management functions are identified.

Audit: FDP_ACF_EXT.1

There are no auditable events foreseen.

FDP_ACF_EXT.1 Local and Session Storage Separation

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_ACF_EXT.1.1

The TSF shall separate local (permanent) and session (ephemeral) storage based on domain, protocol, and port:

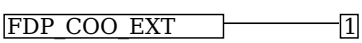
- Session storage shall be accessible only from the originating window/tab;
- Local storage shall only be accessible from windows/tabs running the same web application.

C.2.2 FDP_COO_EXT Cookie Blocking

Family Behavior

Components in this family define requirements for controlling whether or not the TOE stores third-party cookie data.

Component Leveling



FDP_COO_EXT.1, Cookie Blocking, requires the TSF to have a configurable mechanism for blocking the storage of third-party cookies.

Management: FDP_COO_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable storage of third-party cookies.

Audit: FDP_COO_EXT.1

There are no auditable events foreseen.

FDP_COO_EXT.1 Cookie Blocking

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_COO_EXT.1.1

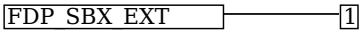
The TSF shall provide the capability to block the storage of third-party cookies by websites.

C.2.3 FDP_SBX_EXT Sandboxing

Family Behavior

Components in this family define requirements for ensuring domain separation through sandboxing.

Component Leveling



FDP_SBX_EXT.1, Sandboxing of Rendering Processes, requires the TSF to implement sandboxing of rendering processes such that least privilege is enforced on the rendering process.

Management: FDP_SBX_EXT.1

No specific management functions are identified.

Audit: FDP_SBX_EXT.1

There are no auditable events foreseen.

FDP_SBX_EXT.1 Sandboxing of Rendering Processes

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_SBX_EXT.1.1

The TSF shall ensure that web page rendering is performed in a process that is restricted in the following manner:

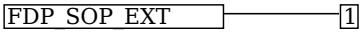
- The rendering process can only directly access the area of the file system dedicated to the browser.
- The rendering process can only directly invoke inter-process communication mechanisms with its own browser processes.
- The rendering process has reduced privilege with respect to other browser processes [**selection**: *[**assignment**: other methods by which the principle of least privilege is implemented for rendering processes], in no other ways*].

C.2.4 FDP_SOP_EXT Same Origin Policy

Family Behavior

Components in this family define requirements for implementation of the Same Origin Policy concept.

Component Leveling



FDP_SOP_EXT.1, Same Origin Policy, requires the TSF to implement the Same Origin Policy concept for web content.

Management: FDP_SOP_EXT.1

No specific management functions are identified.

Audit: FDP_SOP_EXT.1

There are no auditable events foreseen.

FDP_SOP_EXT.1 Same Origin Policy

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_SOP_EXT.1.1

The TSF shall only permit scripts contained in one web page to access data in a second web page if both pages are from the same origin.

FDP_SOP_EXT.1.2

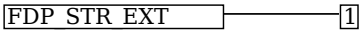
The TSF shall enforce the same origin policy for all domains.

C.2.5 FDP_STR_EXT Secure Transmission of Cookie Data

Family Behavior

Components in this family define requirements for using HTTPS to transmit sensitive cookie data.

Component Leveling



FDP_STR_EXT.1, Secure Transmission of Cookie Data, requires the TSF to use HTTPS to transmit cookie data that has a security-relevant attribute.

Management: FDP_STR_EXT.1

No specific management functions are identified.

Audit: FDP_STR_EXT.1

There are no auditable events foreseen.

FDP_STR_EXT.1 Secure Transmission of Cookie Data

Hierarchical to: No other components.

Dependencies to: FCS_HTTPS_EXT.1 HTTPS Protocol

FDP_STR_EXT.1.1

The TSF shall ensure that cookies containing the 'secure' attribute in the set-cookie header are sent over HTTPS.

C.2.6 FDP_TRK_EXT Tracking Information Collection

Family Behavior

Components in this family define requirements for notifying a user when certain data that reflects the usage of the TOE is being tracked.

Component Leveling

FDP_TRK_EXT.1, Tracking Information Collection, requires the TSF to specify the data tracking that results in user notification.

Management: FDP_TRK_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable ability for websites to collect tracking information about the user.
- Enable/disable deletion of stored browsing data.

Audit: FDP_TRK_EXT.1

There are no auditable events foreseen.

FDP_TRK_EXT.1 Tracking Information Collection

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_TRK_EXT.1.1

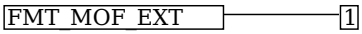
The TSF shall provide notification to the user when tracking information for [**assignment**: *list of trackable browser data*] is requested by a website.

C.2.7 FMT_MOF_EXT Management of Functions Behavior

Family Behavior

Components in this family define requirements for technology-specific management functions that are not enumerated in the Part 2 family FMT_MOF.

Component Leveling



FMT_MOF_EXT.1, Management of Functions Behavior, requires the TSF to implement management functions specified in the SFR.

Management: FMT_MOF_EXT.1

No specific management functions are identified.

Audit: FMT_MOF_EXT.1

There are no auditable events foreseen.

FMT_MOF_EXT.1 Management of Functions Behavior

Hierarchical to: No other components.

Dependencies to: No dependencies.

FMT_MOF_EXT.1.1

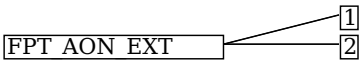
The TSF shall be capable of performing the following management functions, controlled by the administrator or user as shown: [**assignment**: *list of management functions to be performed by role*].

C.2.8 FPT_AON_EXT Add-Ons

Family Behavior

Components in this family define requirements for the secure handling of add-ons that can be installed on top of the TOE.

Component Leveling



FPT_AON_EXT.1, Support for Only Trusted Add-ons, requires the TSF to either support no add-ons or to only support trusted add-ons.

Management: FPT_AON_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable support for add-ons.

Audit: FPT_AON_EXT.1

There are no auditable events foreseen.

FPT_AON_EXT.1 Support for Only Trusted Add-ons

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_AON_EXT.1.1

The TSF shall include the capability to load [**selection**: *trusted add-ons*, *no add-ons*].

FPT_AON_EXT.2, Trusted Installation and Update for Add-ons, requires the TSF to implement a method to verify the integrity of add-ons and ensure that untrusted or unknown add-ons are not loaded for use.

Management: FPT_AON_EXT.2

No specific management functions are identified.

Audit: FPT_AON_EXT.2

There are no auditable events foreseen.

FPT_AON_EXT.2 Trusted Installation and Update for Add-ons

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FPT_AON_EXT.1 Support for Only Trusted Add-Ons

FPT_AON_EXT.2.1

The TSF shall [**selection**: *provide the ability*, *leverage the platform*] to provide a means to cryptographically

verify add-ons using a digital signature mechanism and [**selection**: *published hash*, *no other functions*] prior to installation and update.

FPT_AON_EXT.2.2

The TSF shall [**selection**: *provide the ability*, *leverage the platform*] to query the current version of the add-on.

FPT_AON_EXT.2.3

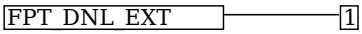
The TSF shall prevent the automatic installation of add-ons.

C.2.9 FPT_DNL_EXT File Downloads

Family Behavior

Components in this family define requirements for downloaded content.

Component Leveling



FPT_DNL_EXT.1, File Downloads, requires the TSF to intervene in the case it is prompted to download executable file data.

Management: FPT_DNL_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable user's ability to select default actions upon download of a file (e.g., always open, or always save, a downloaded file).
- Enable/disable launching of downloaded files outside the browser.

Audit: FPT_DNL_EXT.1

There are no auditable events foreseen.

FPT_DNL_EXT.1 File Downloads

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_DNL_EXT.1.1

The TSF shall prevent downloaded content from launching automatically.

FPT_DNL_EXT.1.2

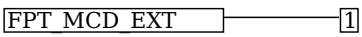
The TSF shall present the user with the option to either save or discard downloaded files.

C.2.10 FPT_MCD_EXT Mobile Code

Family Behavior

Components in this family define requirements for execution of mobile code.

Component Leveling



FPT_MCD_EXT.1, Mobile Code, requires the TSF to identify the mobile code types it supports and to ensure that a mechanism exists to prevent the automatic execution of potentially malicious mobile code.

Management: FPT_MCD_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable display notification when unsigned, untrusted, or unverified mobile code is encountered.
- Enable/disable support for mobile code.

Audit: FPT_MCD_EXT.1

There are no auditable events foreseen.

FPT_MCD_EXT.1 Mobile Code

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_MCD_EXT.1.1

The TSF shall support the capability to execute [**selection**: *signed [**assignment**: supported mobile code*

types] , *no*] mobile code.

FPT_MCD_EXT.1.2

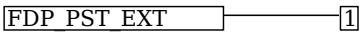
The TSF shall [**selection**: *automatically discard*, *provide the user with the option to discard*] unsigned, untrusted, or unverified [**assignment**: *supported mobile code types*] mobile code without executing it.

C.2.11 FDP_PST_EXT Storage of Persistent Information

Family Behavior

Components in this family define requirements for the minimum amount of information that may be stored persistently by the TSF while retaining its functionality.

Component Leveling



FDP_PST_EXT.1, Storage of Persistent Information, requires the TSF to enumerate the minimum set of data that it must store persistently in order to function normally.

Management: FDP_PST_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable storage of sensitive information in persistent storage.

Audit: FDP_PST_EXT.1

There are no auditable events foreseen.

FDP_PST_EXT.1 Storage of Persistent Information

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_PST_EXT.1.1

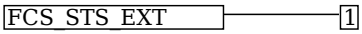
The TSF shall provide the capability to operate without storing persistent data to the file system with the following exceptions: [**assignment**: *data that the TSF must store persistently*].

C.2.12 FCS_STS_EXT Strict Transport Security

Family Behavior

Components in this family define requirements for the implementation of HTTP Strict-Transport-Security.

Component Leveling



FCS_STS_EXT.1, Strict Transport Security, requires the TSF to implement HTTP Strict-Transport-Security.

Management: FCS_STS_EXT.1

The following actions could be considered for the management functions in FMT:

- Enable/disable HSTS mode.

Audit: FCS_STS_EXT.1

There are no auditable events foreseen.

FCS_STS_EXT.1 Strict Transport Security

Hierarchical to: No other components.

Dependencies to: FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_STS_EXT.1.1

The TSF shall implement HTTP Strict-Transport-Security according to RFC 6797.

FCS_STS_EXT.1.2

The TSF shall retain persistent data signaling HSTS enablement for the time span declared by the website in a max-age directive.

FCS_STS_EXT.1.3

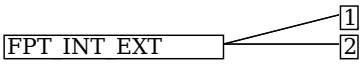
The TSF shall cache the "freshest" Strict Security policy information.

C.2.13 FPT_INT_EXT Reputation Service Interaction

Family Behavior

Components in this family define requirements for the TOE's interaction with reputation services that can provide an assessment of the trustworthiness of data presented to the TSF.

Component Leveling



FPT_INT_EXT.1, Interactions with Application Reputation Services, requires the TSF to be able to interact with an application reputation service to assess whether application data is potentially malicious.

Management: FPT_INT_EXT.1

The following actions could be considered for the management functions in FMT:

- Configure the use of an application reputation service to detect malicious applications prior to download.

Audit: FPT_INT_EXT.1

There are no auditable events foreseen.

FPT_INT_EXT.1 Interactions with Application Reputation Services

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_INT_EXT.1.1

The TSF shall use an application reputation service to prevent downloading of malicious applications.
FPT_INT_EXT.2, Interactions with URL Reputation Services, requires the TSF to be able to interact with a URL reputation service to assess whether websites are potentially malicious.

Management: FPT_INT_EXT.2

The following actions could be considered for the management functions in FMT:

- Configure the use of a URL reputation service to detect sites that contain malware or phishing content.

Audit: FPT_INT_EXT.2

There are no auditable events foreseen.

FPT_INT_EXT.2 Interactions with URL Reputation Services

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_INT_EXT.2.1

The TSF shall use a URL reputation service to prevent connections with malicious websites.

Appendix D - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PP.

Appendix E - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
CRL	Certificate Revocation List
CSRF	Cross-Site Request Forgery
GPU	Graphics Processing Unit
HSTS	HTTP Strict Transport Security
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IETF	Internet Engineering Task Force
IPC	Inter-Process Communication
OCSP	Online Certificate Status Protocol
OE	Operational Environment
PDF	Portable Document Format
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SaaS	Software as a Service
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
W3C	World Wide Web Consortium
XSS	Cross-Site Scripting

Appendix F - Bibliography

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