# Mapping Between

# Application Software Extended Package for Web Browsers, Version 2.0, 2015-06-16

# and

# NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or PP-Configuration supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to block third-party cookies supports AC-4, but only to the extent that blocking these is part of what the control specifies as "organization-defined information flow control policies."
- **Extended Package.** A TOE that conforms to this EP will also conform to the Protection Profile for Application Software (App PP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. The EP does not modify any of the App PP requirements, so it does not affect the security controls that satisfying those requirements is intended to address.

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| **TOE Security Functional Requirements** | | | | |
| FDP_ACF_EXT.1 | **Local and Session Storage Separation** | AC-3 | **Access Enforcement** | A conformant TOE supports this control by ensuring that access to local and session storage is granted only to the browser instances (windows and tabs) that initiated the use of that storage. |
| FDP_COO_EXT.1 | **Cookie Blocking** | AC-4 | **Information Flow Enforcement** | A conformant TOE supports this control by providing a means to enforce an information flow that prevents data from being stored on the TOE's host system based on its origin. |
| FDP_SBX_EXT.1 | **Sandboxing of Rendering Processes** | CM-7 | **Least Privilege** | A conformant TOE supports this control by ensuring that rendering processes has its access constrained to the minimum level needed to perform the rendering. Note that this does not require the browser to operate in a confined physical or virtual environment, so sub-controls CM-7(6) and CM-7(7) do not necessarily apply. |
| FDP_SOP_EXT.1 | **Same Origin Policy** | AC-3 | **Access Enforcement** | A conformant TOE supports this control by enforcing restrictions on the data that a script is allowed to access. |
| FDP_STR_EXT.1 | **Secure Transmission of Cookie Data** | SC-8 | **Transmission Confidentiality and Integrity** | A conformant TOE supports this control by implementing a mechanism to protect the confidentiality of data in transit. |
| | | SC-8(1) | **Transmission Confidentiality and Integrity:** Cryptographic Protection | A conformant TOE supports this control by implementing a cryptographic mechanism (HTTPS) for ensuring the confidentiality of data in transit. |
| FDP_TRK_EXT.1 | **Tracking Information Collection** | PT-4 | **Consent** | A conformant TOE supports this control by notifying the user when their activity is |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| | | | | being tracked so that the user can give consent to this behavior by proceeding with the activity. |
| | | PT-5 | **Privacy Notice** | A conformant TOE supports this control by notifying the user when their behavior is tracked so that the user has sufficient information to determine the extent to which their system activity is private. |
| FMT_MOF_EXT.1 | **Management of Functions Behavior** | AC-3 | **Access Enforcement** | A conformant TOE will not permit manipulation of its functional behavior unless proper authorization is provided. |
| | | AC-3(7) | **Access Enforcement:** Role-Based Access Control | A conformant TOE will restrict access to management functionality to members of a certain role. |
| | | AC-6 | **Least Privilege** | A conformant TOE enforces least privilege by restricting the users that are able to manage TSF functionality. |
| | | CM-6 | **Configuration Settings** | A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE. |
| FPT_DNL_EXT.1 | **File Downloads** | CM-7(2) | **Least Functionality:** Prevent Program Execution | A conformant TOE supports this control by ensuring that downloaded executable code is not launched without explicit user authorization. |
| FPT_MCD_EXT.1 | **Mobile Code** | SC-18 | **Mobile Code** | A conformant TOE supports part (b) of this control by |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| | | | | providing the ability to prevent the use of untrusted mobile code. |
| | | SC-18(4) | **Mobile Code:** Prevent Automatic Execution | A conformant TOE supports this control by prompting the user to authorize the execution of untrusted mobile code rather than allowing it to run automatically. |
| FPT_AON_EXT.1 | **Support for Only Trusted Add-ons** | CM-14 | **Signed Components** | A conformant TOE supports this control by ensuring that add-ons are not supported unless explicitly trusted, which is achieved through the add-on's use of a digital signature. |
| **Optional Requirements** | | | | |
| FDP_PST_EXT.1 | **Storage of Persistent Information** | N/A | **N/A** | This SFR requires the TOE to be able to operate in a way that minimizes the persistent information that it needs to store so as to limit the potential for unauthorized access to that information. There are no security controls that this behavior applies to specifically. |
| **Selection-Based Requirements** | | | | |
| FPT_AON_EXT.2 | **Trusted Installation and Update for Add-ons** | CM-14 | **Signed Components** | A conformant TOE requires that updates to its add-ons include integrity measures. Depending on the selection made in the SFR, this may include a digital signature.<br><br>Note that the SFR also prohibits the automatic installation of add-ons but there are no controls that this behavior applies to. |
| | | SI-7(1) | **Software, Firmware, and Information Integrity:** Integrity Checks | A conformant TOE has the ability to verify the integrity of any add-ons that are installed on top of it. |
| **Objective Requirements** | | | | |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| FCS_STS_EXT.1 | **Strict Transport Security** | SC-8 | **Transmission Confidentiality and Integrity** | A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted to and from the TOE by forcing the use of HTTPS through implementation of HSTS. |
| | | SC-8 (1) | **Transmission Confidentiality and Integrity:** Cryptographic Protection | A conformant TOE supports this control by forcing the use of a cryptographic mechanism (HTTPS) for securing data in transit. |
| FPT_INT_EXT.1 | **Interactions with Application Reputation Services** | CM-11 | **User-Installed Software** | A conformant TOE supports part (b) of this control by providing a mechanism to enforce restrictions on the software that users can install. |
| | | SI-3 | **Malicious Code Protection** | A conformant TOE supports part (a) of this control by implementing a mechanism to flag downloaded applications as potentially malicious. |
| FPT_INT_EXT.2 | **Interactions with URL Reputation Services** | SI-3 | **Malicious Code Protection** | A conformant TOE supports part (a) of this control by implementing a mechanism to flag websites as potential sources of malicious code. |