

UNCLASSIFIED



**DoD ANNEX
FOR
PROTECTION PROFILE FOR APPLICATION
SOFTWARE V1.1**

Version 1, Release 3

23 October 2015

Developed by DISA for the DoD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

REVISION HISTORY

| Version | Date | Description |
|----------------|-----------------|---|
| 1.1 | 16 April 2015 | Initial Release |
| 1.2 | 18 May 2015 | Updated section 1.1 to state the Annex applies to version 1.1 of the protection profile. |
| 1.3 | 27 October 2015 | Added a new list of DoD-required selection-based SFRs to support the DoD Annex to the Browser EP (see section 2.2 and Table 2-2). |

TABLE OF CONTENTS

| | Page |
|---|-------------|
| 1. INTRODUCTION..... | 1 |
| 1.1 Background | 1 |
| 1.2 Scope | 1 |
| 1.3 Mobile Application Vetting | 2 |
| 1.4 Relationship to Security Technical Implementation Guides (STIGs)..... | 2 |
| 1.5 Document Revisions | 3 |
| 2. DOD-MANDATED SECURITY TARGET CONTENT | 4 |
| 2.1 DoD-Mandated Assignments and Selections | 4 |
| 2.2 DoD-Mandated Optional, Selection-Based, and Objective SFRs..... | 5 |
| 3. OTHER DOD MANDATES | 6 |
| 3.1 Federal Information Processing Standard (FIPS) 140-2 | 6 |
| 3.2 Federal Information Processing Standard (FIPS) 201-2 | 6 |
| 3.3 DoD-Mandated Configuration | 6 |

LIST OF TABLES

| | Page |
|--|-------------|
| Table 2-1: PP SFR Selections | 4 |
| Table 2-2: PP SFR Selections for Optional, Selection-Based, and Objective SFRs | 5 |
| Table 3-1: Configuration Values | 6 |

1. INTRODUCTION

1.1 Background

This Annex to the Protection Profile (PP) for Application Software (Version 1.1, dated 06 November 2014) delineates PP content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated PP selections and assignments, and PP security functional requirements (SFRs) listed as optional or objective in the PP but which are mandated in the DoD. As stated in DoD Instruction 8500.01 "Cybersecurity, NIAP evaluation is expected for IA and IA-enabled products in accordance with CNSSP 11. Evaluation of applications without IA functionality is at the discretion of the Authorizing Official."

Deficiencies of the TOE with respect to the DoD Annex will be reported as appropriate under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to the DoD. Accordingly, any vendor seeking authorization for use of its product within the DoD should include the additional PP specificity described in this Annex in its ST.

The PP for APP SW, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Taken together, they supersede the DoD Mobile Application Security Requirements Guide.

1.2 Scope

The additional information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

STIGs will NOT be developed for most mobile applications. A STIG will be developed under the following conditions:

- The mobile application is an Information Assurance (IA) or IA-enabled product in a National Security System (NSS), and therefore subject to the Committee on National Security Systems Policy (CNSSP) 11 requirement that the product be evaluated against a National Information Assurance Partnership (NIAP)-approved protection profile;
- The mobile application poses an unacceptable risk to DoD information or information systems without configuration; and
- The risk of operating the mobile application without configuration cannot be sufficiently mitigated by the required controls in the relevant mobile operating system STIG.

NIAP will determine whether the first criterion is satisfied. The Authorizing Official (AO) responsible for the mobile system will determine whether the remaining criteria are satisfied.

1.3 Mobile Application Vetting

App vetting refers to a process for evaluating the security of apps [1]. AOs must decide upon a vetting process for their organization. All vetting processes within DoD are expected to use the NIAP Protection Profile for Application Software as a baseline, in addition to this Annex. Their requirements provide a basis for decision-making by AOs who must weigh risks and then decide between using commercial app stores and investing in organizational app vetting services. IA and IA-enabled applications on National Security Systems must undergo formal NIAP evaluation in accordance with CNSS Policy #11 [2].

Many mobile applications are bundled with a mobile operating system (i.e., they are not separately-installed third-party applications). A core app is defined as an app bundled by the operating system vendor (for example Google, Apple, Microsoft, or BlackBerry). A pre-installed app is included on the device by a third-party integrator, including the device manufacturer or cellular service provider (for example LG, Samsung, Verizon Wireless, or AT&T). Core applications and pre-installed applications must be vetted. When core and pre-installed applications receive a negative disposition in application vetting, the underlying operating system must be configured to disable the application wherever feasible.

1.4 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in eXtensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

This Annex contains the required DoD configuration of features implementing the Security Management (FMT) class of SFRs listed in the PP for APP SW. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG. A STIG includes all security parameters under the control of the user or administrator, indicating secure values as appropriate. Additional configuration requirements for more-specialized applications may also be captured in DoD Annexes to Extended Packages of the APP SW PP.

[1] NIST Special Publication 800-163 "Vetting the Security of Mobile Applications"
<http://csrc.nist.gov/publications/PubsSPs.html>

[2] National Information Assurance Partnership "Usage of the Protection Profile for Application Software"
https://www.niap-ccevs.org/pp/PP_APP_v1.1/

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to:
disa.stig_spt@mail.mil.

2. DOD-MANDATED SECURITY TARGET CONTENT

The following conventions are used to describe DoD-mandated ST content:

- If a PP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For PP selections:
 - The presence of the selection indicates this is a DoD-mandated selection.
 - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
 - Underlined text indicates a selection.
 - *Italicized and underlined* text indicates an assignment within a selection.
 - ~~Strikethrough~~ text indicates that the ST author must exclude the selection.
- For PP assignments:
 - The DoD-mandated assignments are listed after the assignment parameter.
 - If an assignment value appears in ~~strikethrough~~ text, this indicates that the assignment must not include this value.
 - *Italicized* text indicates an assignment.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the PP for APP SW and the DoD Annex simultaneously to place the Annex information in context.

2.1 DoD-Mandated Assignments and Selections

DoD mandates the following PP SFR selections and assignments for SFRs in Section 4 of the PP for APP SW.

Table 2-1: PP SFR Selections

| SFR | Selections, Assignments, and Application Notes |
|-----------|--|
| FMT_SMF.1 | <p><i>list of other management functions to be provided by the TSF = deny all inbound UDP/TCP traffic except traffic on [assignment: list of TCP/UDP ports].</i></p> <p>Application note: The mobile app must utilize ports or protocols in a manner consistent with DoD Ports and Protocols guidance, including the DoD Ports Protocols Services Management (PPSM) Category Assurance List (CAL). If it does so natively, this management functionality is not required. If it does not do so, then it must permit configuration to obtain a state consistent with the PPSM CAL.</p> |

2.2 DoD-Mandated Optional, Selection-Based, and Objective SFRs

The following SFRs (and associated selections and assignments) listed as objective in the PP are mandated for the DoD to support the DoD Annex for the Browser EP:

- FIA_X509_EXT.1.1
- FIA_X509_EXT.2.1
- FIA_X509_EXT.2.2
- FPT_TUD_EXT.1.1
- FPT_TUD_EXT.1.2
- FPT_TUD_EXT.1.3
- FPT_TUD_EXT.1.4
- FPT_TUD_EXT.1.5

Table 2-2: PP SFR Selections for Optional, Selection-Based, and Objective SFRs

| SFR | Selections, Assignments, and Application Notes |
|------------------|--|
| FIA_X509_EXT.1.1 | <p><u>the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759</u></p> <p>Note: An ST that includes a CRL selection is acceptable if it also selects OSCP and provides a management functionality to require OSCP over CRL.</p> |
| FIA_X509_EXT.2.1 | <u>HTTPS, TLS, DTLS</u> |
| FIA_X509_EXT.2.2 | <u>allow the administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate</u> |
| FPT_TUD_EXT.1.1 | <u>provide the ability, leverage the platform</u> |
| FPT_TUD_EXT.1.5 | <u>provide the ability, leverage the platform</u> |

3. OTHER DOD MANDATES

3.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS140-2 validated. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation could preclude use of the TOE within DoD.

3.2 Federal Information Processing Standard (FIPS) 201-2

Where the TOE supports authentication to remote DoD servers, it is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST 800-157) provided by the TOE platform. The TOE platform may connect to a peripheral (e.g., a smart card reader).

3.3 DoD-Mandated Configuration

The table below lists configuration values for product features implementing the PP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information, but it will be included in the product-specific STIG associated with the evaluated IT product. Non-binary configuration values are shown in *italics*.

Table 3-1: Configuration Values

| FMT_SMF_EXT.1 Function | DoD Selections and Values |
|---------------------------|--|
| FMT_SMF.1.1 | <i>[assignment: list of DoD-approved TCP/UDP ports included in the DoD Ports Protocols Services Management (PPSM) Category Assurance List (CAL)]</i> |