Network Device Protection Profile Extended Package
SIP Server

5 November 2014

Version 1.1

Table of Contents

Revision History

Version	Date	Description
1.0	*06 February 2013*	Initial release
1.1	*November 2014*	Updated TLS requirement to include additional optional cipher suites.

1 INTRODUCTION

This Extended Package (EP) describes the security requirements for a Session Initiation Protocol (SIP) Server and provides a minimal baseline set of requirements targeted at mitigating well defined threats. However, this EP is not complete in itself, but rather extends the *Security Requirements for Network Devices* protection profile (NDPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDPP.

Since this PP is designated for the SIP Server, is should be understood that the Target of Evaluation (TOE) is the SIP server and "SIP server" and "TOE" are used interchangeably within this document.

1.1 Conformance Claims

The *Security Requirements for Network Devices* Protection Profile (NDPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDPP baseline with additional SFRs and associated 'Assurance Activities' specific to SIP Server network infrastructure devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

As an EP of the NDPP, it is expected that the content of both this EP and the NDPP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in so doing. An ST must identify the applicable versions of the NDPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

1.3 First Generation Mobility Profiles

What makes security for mobility different than other technologies? Regardless of the actual technical security features of individual devices, a wired computing or communications device has implied security if the physical environment where the device resides is protected by guards, dogs and fences. For mobility, these traditional physical protections are irrelevant. Not only are the wireless communications channels more readily available to adversaries, but the devices themselves are also expected to be multipurpose and used for both work and enterprise data. Mobility clearly brings new security challenges.

To keep up with the rapidly-evolving mobility market place, the Information Assurance Directorate (IAD) intends to manage the risks of missing or imperfectly implemented mobility security features by issuing the first generation Mobility PPs and EPs. These first generation Mobility Profiles will be a mechanism to select from a pool of commercial products with the security features IAD requires. An aggressive timeline is necessary since vendors are already requesting to participate in mobility efforts, and because of IAD deadlines for implementing first generation solutions. The first generation Mobility Profiles will consist of the Mobile OS PP, SIP Server EP (this document), and the Mobility App (VOIP) PP. The goal of

these PPs and EP is to present current requirements and what is possible today so that a clear direction is taken for security critical components to provide better enterprise security.

Some desired mobility security features might not be reasonably expected to appear within the next eighteen months. Those features that go beyond where commercial industry is currently heading will probably not be supported by interim mobility solutions, or by the first generation Mobility Profiles. IAD will work with vendors to determine how and when to obtain products with these features, and whether /when to create the corresponding PPs and EPs.

1.4 Compliant Targets of Evaluation

This is a EP for a SIP Server. The Voice over IP (VoIP) infrastructure for an enterprise can vary greatly, both in size and complexity. Many kinds of functionality are possible, often desirable, and sometimes necessary – including Session Border Controllers (SBC), gateways, trunking, Network Address Translation (NAT), and firewall traversal. The SIP Server interacts with a VoIP client and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls. As a registered server, the SIP server accepts REGISTER requests and places the information received into the location service on the server. As a SIP proxy server, the server is a stateful server that manages transactions to route SIP requests and responses.

While the functionality that the TOE is obligated to implement in response to the described threat environment is discussed in detail in later sections, it is useful to give a brief description here. A compliant TOE will provide security functionality that addresses threats to itself. It must also protect communications between itself and a VoIP client (i.e., smartphone) or another SIP server by using a TLS protected channel. As a registrar server, the SIP server will require user/password authentication of the SIP user for SIP REGISTER. The protocols required by this PP make use of certificates so the SIP server must securely store certificates and private keys. As shown in Figure 1, the SIP server communicates with the VoIP clients over a protected Transport Layer Security (TLS) channel. Components in red are addressed in this PP. Components in blue are addressed in related PPs.

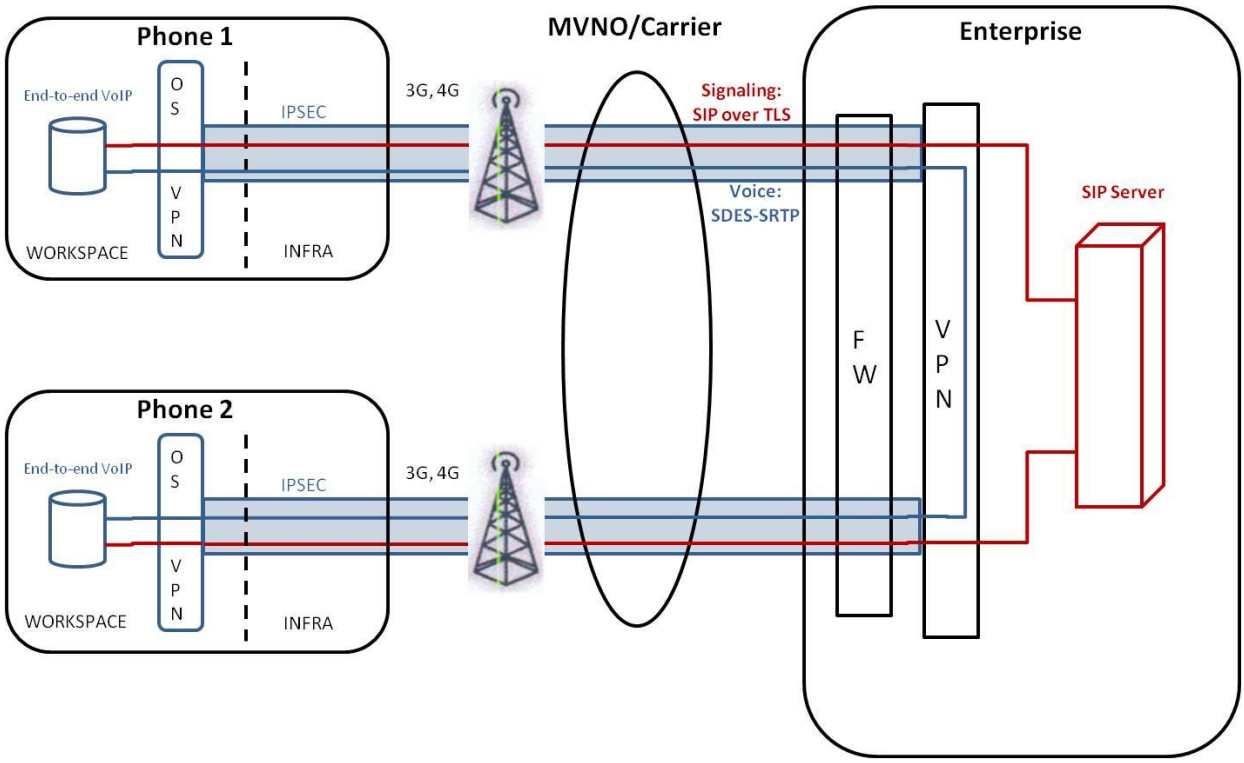

Figure 1: VoIP Communications

Since this EP builds on the NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

The set of requirements in this EP is purposely limited in scope in order to promote quicker, less costly evaluations that provide some value to end users. Security Targets (ST) that include a large amount of additional functionality (and requirements) are discouraged.

2 SECURITY PROBLEM DESCRIPTION

The SIP server must address threats and policies that are common to a SIP server in general rather than those that might be targeted at a specific SIP server function or at a specific type of SIP server. Annex A presents the Security Problem Description (SPD) in a more “traditional” form. The following sections detail the problems that compliant TOEs will address; references to the “traditional” statements in Annex A are included.

Note that this EP does not repeat the threats identified in the NDPP, though they all apply given the conformance and hence dependence of this EP on the NDPP. Note also that while the NDPP contains only threats to the ability of the TOE to provide its security functions, this EP addresses only business threats to resources in the operational environment. Together the threats of the NDPP and those defined in this EP define the comprehensive set of security threats addressed by a VPN TOE.

2.1 Communications with the TOE

SIP servers communicate with other SIP servers, VoIP clients, as well as administrators, over communication networks. The endpoints can be both geographically and logically separated from the SIP server, and pass through a variety of other systems which may be under the control of an adversary, and offer the opportunity for communications with the SIP server to be compromised. Although a VPN tunnel provides a layer of security for the TOE to communicate with the Enterprise, additional layers of security are needed to protect call control traffic and Real Time Services media streams.

Unencrypted communications with the SIP server may allow critical data such as passwords, keys, configuration settings, and routing updates, to be read and/or manipulated directly by intermediate systems, leading to a compromise of the server. Several protocols can be used to provide protection. However, these protocols have many configurable options that can be used to customize each protocol yet still allow it to remain compliant to its specification. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm, even one that is allowed by the RFC, could allow an adversary to read or manipulate the data on the encrypted channel, thus circumventing countermeasures put in place to prevent such attacks. Further, if the protocol is implemented with rarely used or non-standard options, it may be compliant with the protocol specification but may be non-interoperable with other equipment using the same protocol.

Even though the communication path is protected, it is possible that an external entity such as a mobile device application, another SIP server, or a trusted IT entity such as a peer router could be deceived into thinking that a malicious attacker is the SIP server. In a similar manner, the SIP server could be fooled into thinking that it is establishing communications with a legitimate remote entity when in fact, it isn't. An attacker could mount a man-in-the-middle attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by the compromised system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. Some of these attacks happen when an attacker captures a segment of traffic such as an authentication session and reuses the traffic in order to fool an endpoint into thinking it was communicating with a valid remote entity.

[T.UNAUTHORIZED_ACCESS]

3 SECURITY OBJECTIVES

The SIP server will provide security functionality that address threats to it and implement policies that are imposed by law or regulation. The following sections provide a description of this functionality. The security functionality focuses on protected communications between elements of the server and the VoIP clients. The description of that security objectives are in addition to that described in [NDPP].

3.1 Protected Communications

To address the issues concerning transmitting sensitive data to and from the SIP server described in Section 2.1, the server will encrypt the communication paths between itself and the endpoints. These communication channels are implemented using TLS. TLS provides interoperability and resistance to attack. The SIP server must support TLS, but they may also support additional algorithms and protocols. Whether these additional algorithms and protocols will be evaluated is Scheme-dependent. If they are not evaluated, the administrator must be informed so that they can be disabled or shown not to affect the specified security functionality during server operations.

In addition to providing protection from disclosure and detection of modification for the communications, the TLS protocol offers two-way authentication of each endpoint in a cryptographically secure manner. This means if an attacker located between the two endpoints tries to pretend to be one of the communicating parties, the attempt would be detected. The TLS protocol also provides protection against replay attacks such as those described in Section 2.1. This is done by including a unique value in each communication, such as a timestamp, so that an attempt to replay the communication would be detected.

(FCS_CKM.1(*), FCS_CKM_EXT.4, FCS_COP.1(*), FCS_TLS_EXT.1, FCS_RBG_EXT.1, FIA_SIPS_EXT.1, FIA_X509_EXT.1, FTP_ITC.1(*))

3.2 System Monitoring

To address the issues of administrators being able to monitor the operations of the SIP Server, this security objective, which originated in the NDPP, is extended as follows.

Compliant TOEs will implement the ability to log the establishment of the TLS session, and the establishment of the SIP session.

(FAU_GEN.1)

3.3 TOE Administration

To address the issues involved with a trusted means of administration of the VPN gateway, this security objective, which originated in the NDPP, is extended as follows.

Compliant TOEs will provide the functions necessary for an administrator to configure the cryptographic aspects of the TLS connection, as well as the required aspects of the SIP implementation for operation with SIP clients.

(FMT_SMF.1)

4 SECURITY REQUIREMENTS

The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3*, with additional extended functional components.

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated by the word "Refinement" in **bold text** after the element number with additional text in **bold** text and deletions with strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

4.2 TOE Security Functional Requirements

4.2.1 NDPP Security Functional Requirement Direction

This section instructs the ST Author what selections must be made to certain SFRs contained in the NDPP in order to support related SFRs in the SIP Server EP. This is captured by expressing the element where the mandatory selection has been made. The ST Author may complete the remaining selection items as they wish. To ensure specific capabilities or behavior is present in the TOE selections in SFR elements have been made as well.

Assurance activities are not repeated for the requirements in this section, as those are already captured in the NDPP. What is important for the evaluator when they assess the ST and TOE against the SFRs as specified here is that the proper selections have been made and the appropriate tests are performed to demonstrate compliance to the requirements.

FCS_COP.1(1) Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1 The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in GCM, [assignment: one or more modes]* and cryptographic key sizes *128-bits, 256-bits, and [selection: 192 bits, no other key sizes]* that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- *[selection: NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP 800-38E]*

Application Note:

This EP requires the GCM mode to be used in the TLS protocol (FCS_TLS_EXT.1). Therefore, the FCS_COP.1.1(1) element in the NDPP has been specified here to ensure the ST Author includes this mode to be consistent with the TLS requirements. The ST author is expected to add other appropriate modes to support the remote administrative requirements of the NDPP.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

a. *Ability to configure the SIP;*
b. *Ability to configure mechanisms implemented with respect to FCS_TLS_EXT.1;*
c. *Ability to configure SIP client password;*
d. *Ability to configure a notice and consent warning message for FTA_TAB.1.*
e. *Ability to configure inactivity time period for local sessions time period for FTA_SSL_EXT.1.*

Application Note:

The elements listed above are to be combined with the elements in the NDPP selected by the ST author to formulate the entire set of management functions implemented by the TOE.

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: published hash, no other functions] prior to installing those updates.

Application Note:

The NDPP provides an option of which method of verification the ST Author wishes to specify. For compliance with this EP, a digital signature mechanism (one of those specified in FCS_COP.1(2) must be employed. Note that the ST author should include the other two elements of the NDPP FPT_TUD_EXT.1 in the ST.

4.2.2 Cryptographic Support (FCS)

In this and subsequent sections, requirements levied on the TOE by this EP that are not contained in the NDPP are defined.

FCS_TLS_EXT.1 Transport Level Security

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] using mutual authentication with certificates and supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites: [*selection:*

- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 6460*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 6460*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *no other ciphersuite*]

Application Note:

The ciphersuites to be used in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE.

The Suite B algorithms (RFC 6460) listed above are the preferred algorithms for implementation.

In a future version of this PP, TLS v1.2 will be required for all TOEs.

Assurance Activity:

TSS

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

Test

The evaluator shall also perform the following test:

Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a SIP session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the

encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

4.2.3 Identification and Authentication (FIA)

FIA_SIPS_EXT.1 Session Initiation Protocol (SIP) Server

FIA_SIPS_EXT.1.1 The TSF shall implement the Session Initiation Protocol (SIP) that complies with RFC 3261 using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VOIP traffic.

FIA_SIPS_EXT.1.2 The TSF shall require password authentication for SIP REGISTER function requests as specified in section 22 of RFC 3261.

FIA_SIPS_EXT.1.3 The TSF shall support SIP authentication passwords that contain at least [assignment: positive integer of 8 or more] characters in the set of {upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [assignment: other supported special characters]}.

Application Note:

The only SIP request that is required to be authenticated (by the TOE) is the REGISTER request. The SIP Server will perform the enforcement and only register the user upon the presentation of the correct password; the TOE is required by the elements above to support passwords that are at least 8 characters long (the maximum length is defined in the first assignment) and can contain the characters identified in FIA_SIPS_EXT.1.3 (characters allowed by the TOE but not listed explicitly in the element should be identified in the second assignment; otherwise "no other characters" is an acceptable assignment.

Assurance Activity:

TSS

The evaluator shall examine the TSS to verify that it describes how the SIP session is established. This shall include the initiation of the SIP session, registration of the user, and how both outgoing and incoming calls are handled (initiated, described, and terminated). This description shall also include a description of the handling of the password from the time it is received by the TOE until the time the user is authenticated.

Test

The tests are written from the standpoint of using a client as the distant end of the test; alternative methods showing the same functionality are allowed. The evaluator shall perform the following tests:

Test 1: The evaluator shall follow the procedure for initializing their device to include establishing a connection to the SIP Server. The evaluator shall confirm that they are prompted for a password prior to successfully completing the SIP REGISTER request.

Test 2: The evaluator shall follow the procedure for initializing their device to include establishing a connection to the SIP Server. The evaluator shall confirm that entering an incorrect password results in the device not being registered by the SIP Server (e.g., they are unable to successful place or

receive calls). The evaluator shall also confirm that entering the correct password allows the successful registration of the device (e.g., by being able to place and receive calls).

Test 3: The evaluator shall set up the test environment such that a variety of passwords are shown to be accepted by the TOE, such that the length and character set identified in FIA_SIPC_EXT.1.3 is represented. The test report shall contain a rationale by the evaluator that the test set used is representative of the allowed lengths and characters.

X509 Certificates (FIA_X509_EXT)

The certificates used by the TSF are those for the distant end TLS connection and the user's certificate (and assocaited private key).

FIA_X509_EXT.1 Extended: X.509 Certificates

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

Application Note:

It should be noted that RFC 5280 defines certificate validation and certification path validation requirements that must be implemented by the TOE as per this requirement..

FIA_X509_EXT.1.2 The TSF shall provide the capability for the Enterprise to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

FIA_X509_EXT.1.3 The TSF shall validate the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].

FIA_X509_EXT.1.4 The TSF shall not establish a TLS connection if a certificate is deemed invalid.

FIA_X509_EXT.1.5 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall, as configured by the Enterprise, establish the TLS connection or disallow the establishment of the TLS connection.

FIA_X509_EXT.1.6 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

Application Note:

The intent of FIA_X509_EXT.1.5 is that the TOE is configurable to allow or disallow session establishment if the TOE cannot connect to an entity responsible for providing certificate validation information. For instance, if a CRL cannot be obtained because a machine is down, or the network path is broken, the administrator may elect to configure the TOE to allow sessions to continued to be established, rather than terminate the TOE's ability to establish any new connections because it cannot reach the CA.

Assurance Activity:

TSS

The evaluator shall ensure the TSS describes all certificate stores implemented that contain certificates used to meet the requirements of this EP. This description shall contain information pertaining to how certificates are loaded into storage, and how the storage is protected from unauthorized access.

Guidance

The evaluator shall examine the guidance documentation to ensure it describes how to configure either the TOE or the environment to prevent unauthorized modification or deletion of the certificates.

Test

The evaluator shall perform the following tests for each function in the system that requires the use of certificates:

Test 1: The evaluator shall demonstrate that using a certificate without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.

Additional testing to ensure the requirements are satisfied is performed in conjunction with the TLS requirements in FTP_ITC.1(2).

4.2.4 Trusted Path/Channel (FTP)

FTP_ITC.1(2) Inter-TSF Trusted Channel (TLS/SIP)

FTP_ITC.1.1(2) **Refinement:** The TSF shall provide a communication channel between itself and **a SIP Client using TLS [selection: "and no other protocol", "and DTLS"] as specified in FCS_TLS_EXT.1 [selection: "only", "and in FCS_DTLS_EXT.1"]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and ~~or~~ disclosure.

FTP_ITC.1.2(2) The TSF shall permit the TSF Client to initiate communication via the trusted channel

FTP_ITC.1.3(2) The TSF Client shall initiate communication via the trusted channel for [all communications with the SIP server].

Application Note:

The SIP client will establish a connection with the TOE on start-up, and this will persist as long as the device containing the SIP client is powered on and able to send/receive calls. While the TOE is required to be able to use TLS to establish this connection, DTLS is also allowed. If DTLS is also implemented, then the ST author should make the second of each selection in FTP_ITC.1.1(2); otherwise the first selection will be made. If DTLS is implemented, the DTLS requirement in Annex C will also be moved to the body of the ST.

***Assurance Activity**:*

TSF

The evaluator shall check the TSS section to confirm that it describes how this requirement is implemented in the TOE.

Test

The evaluator shall verify that communication can be initiated from a SIP client.

FTP_ITC.1(3) Inter-TSF Trusted Channel (Protection from Modification or Disclosure – SIP Server)

FTP_ITC.1.1(2) **Refinement:** The TSF shall provide a communication channel between itself and another **SIP Server using [selection: IPsec, SSH, TLS, TLS/HTTPS]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2(2) The TSF shall permit **the TOE or the peer SIP Server** to initiate communication via the trusted channel

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel [*to pass SIP data to a SIP Server Peer*].

Application Note:

This requirement addresses the case where the TOE establishes communications another SIP Server. This channel is required to be protected similar to the remote administrative connection in the NDPP; the protocol selected by the ST author above should be included from the NDPP in the ST.

***Assurance Activity**:*

TSF

The evaluator shall check the TSS section to confirm that it describes how this requirement is implemented in the TOE.

Test

The evaluator shall verify that communication can be initiated from both the TSF and another SIP Server. Additional assurance activities may be required based on the components included from the NDPP.

4.2.5 Security Audit

There are no additional SFRs for security audit. However, there are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the NDPP. As such, the following events should be combined with those of the NDPP in the context of a conforming Security Target.

The following audit events are required for this EP.

4-1 FAU_GEN.1 Audit Event and Details

Requirement	Auditable Events	Additional Audit Record Contents
FCS_TLS_EXT.1	Session Establishment with peer	Source and destination addresses Source and destination ports TOE Interface
FIA_X509_EXT.1	Establishing session with CA	Source and destination addresses Source and destination ports TOE Interface
FIA_SIPS_EXT.1	Session Establishment with peer	Source and destination addresses Source and destination ports TOE Interface

4.3 Security Assurance Requirements

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDPP as well. The NDPP includes a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that similarly refine the SARs associated with the EAL identified in the NDPP. The assurance activities associated with SARs that are prescribed by the NDPP are performed against the entire TOE.

RATIONALE

The rationale tracing the threats to the objectives and the objectives to the requirements is contained in the prose in Sections 2.0 and 3.0. The only outstanding mappings are those for the Assumptions and Organizational Security Policies; those are contained in Annex A below.

ANNEX A: SUPPORTING TABLES

In this Protection Profile, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats to network devices; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this Annex contains the tabular artifacts that can be used for the evaluation activities associated with this document.

Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

PP authors should ensure that the assumptions still hold for their particular technology; the table should be modified as appropriate.

Table 3: TOE Assumptions

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Threats

The following threats should be integrated into the threats that are specific to the technology by the PP authors when including the requirements described in this document. Modifications, omissions, and additions to the requirements may impact this list, so the PP author should modify or delete these threats as appropriate.

Table 4: Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

Security Objectives for the TOE

Table 6: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

The following table contains objectives for the Operational Environment. As assumptions are added to the PP, these objectives should be augmented to reflect such additions.

Table 7: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

ANNEX C: ADDITIONAL REQUIREMENTS

As indicated in the body of this PP, there are several methods by which conformant TOEs can perform certain security functions required to address the objectives. The requirements in the body of the PP indicate those functions that must be implemented by the TSF. There are other functions, however, that are allowed to be implemented by either the TSF or the Mobile OS, or to not be implemented at all. The following sections contain a list of those requirements; if these are implemented by the TSF, then the requirements will be moved by the ST author to the body of the ST.

Note that minor adjustments to the narrative information in the beginning of the ST may be required depending on the selections performed.

C.1.1 Datagram Transport Level Security

SIP through TLS must be implemented by the TOE; however, it is also allowable for DTLS to be implemented in addition to TLS. If DTLS is supported, the following requirement will be included by the ST author.

FCS_DTLS_EXT.1 Extended: Datagram Transport Level Security

FCS_DTLS_EXT.1.1 The TSF shall implement the DTLS protocol in accordance with RFC 6347.

FCS_DTLS_EXT.1.2 The TSF shall implement the requirements in FCS_TLS_EXT.1 for the DTLS implementation, except where variations are allowed according to RFC 6347.

Application Note:

Differences between DTLS and TLS are outlined in RFC 6347; otherwise the protocols are the same. In particular, for the applicable security characteristics defined for the TOE, the two protocols do not differ. Therefore, all application notes and assurance activities that are listed for FCS_TLS_EXT.1 apply to the DTLS implementation.

Assurance Activity:

The evaluator shall perform the assurance activities listed for FCS_TLS_EXT.1 to verify this component