Security Requirements for Voice Over IP Application

Information Assurance Directorate

24 January 2013

Version 0.6

Table of Contents

List of Tables

List of Figures

Revision History

Version	Date	Description
1.0	*<dd month yyyy>*	Initial release

1 INTRODUCTION

1 This Protection Profile (PP), describing security requirements for a Voice over Internet Protocol (VoIP) application, is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. It represents an evolution of "traditional" Protection Profiles and the associated evaluation of the requirements contained within the document. This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss the evolutionary aspects of the PP as a guide to readers of the document.

1.1 First Generation Protection Profiles

2 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 communication 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.

3 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 PPs. The Information Assurance Directorate (IAD) will work with vendors to determine how and when to obtain products with these features, and whether/when to create the corresponding PPs.

1.2 Compliant Targets of Evaluation

4 This is a PP for a VoIP application. The VoIP application in the context of this PP is part of the cell phone workspace that the enterprise can install for use by the phone user. The 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, and Network Address Translation (NAT) and firewall traversal. The VoIP Application in the context of this PP is considered to be a VoIP client that interacts with a SIP Server which provides registrar and proxy capabilities required for call-session management via SIP requests and responses to establish, process, and terminate VoIP calls. The VoIP Application will interact with a peer Application using the Security Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP.

5 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. Compliant TOEs will provide security functionality that addresses threats to the TOE. They must also protect the communications between itself and another VoIP client (i.e., cell phone) by using a SDES-SRTP-protected channel. Likewise, compliant TOEs must also protect communications between itself and the SIP Server by using a Transport Layer Security (TLS)- and (optionally) a Datagram Transport Layer Security (DTLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE is required by this PP to make use of certificates to authenticate the both the SIP server end and the TOE itself through the TLS connection. The TOE must provide the ability to report its version to the Enterprise so that a determination as to whether it can be updated can be made. As shown in Figure 1, the TOE communicates with other VoIP clients and SIP

Servers over protected channels. Components in red are addressed in this PP. Components in blue are addressed in related PPs.

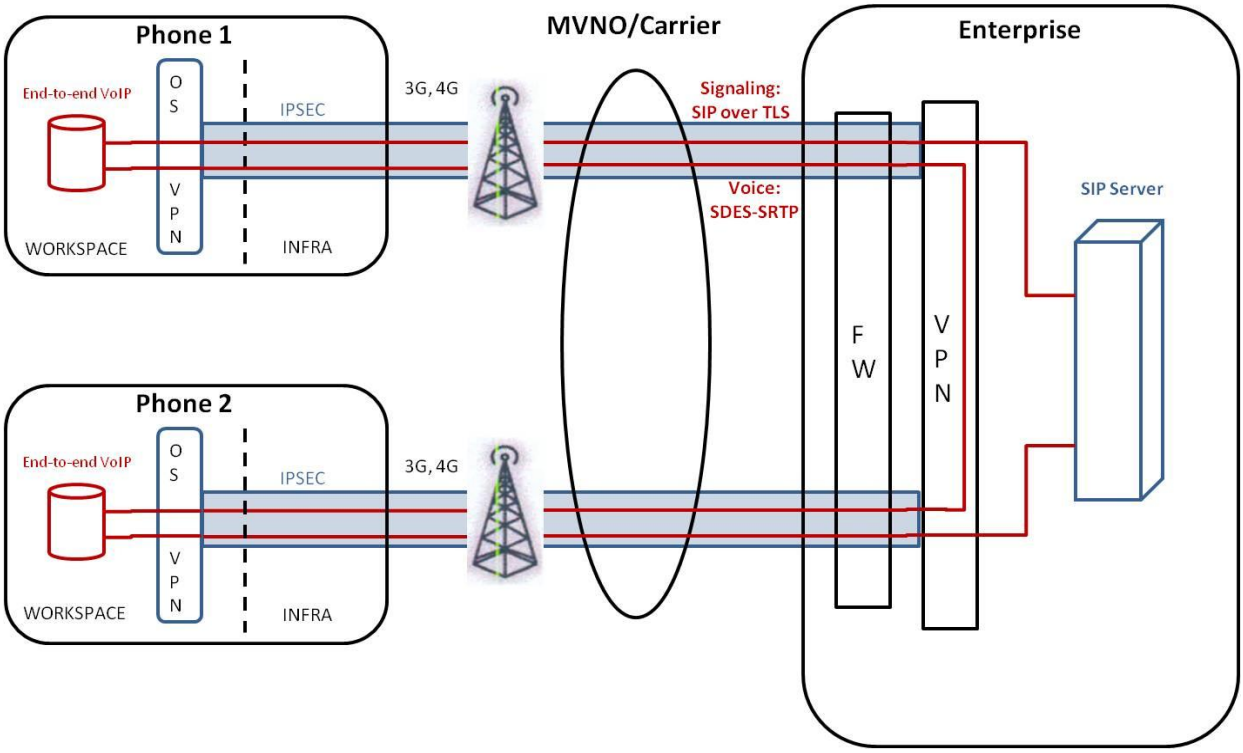

Figure 1: VoIP Communication

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

2 SECURITY PROBLEM DESCRIPTION

7 As detailed in the previous section, the security problem to be addressed by compliant TOEs is described by threats and policies that are common to a mobile VoIP application, as opposed to those that might be targeted at the specific functionality of a specific type of VoIP application. Annex A: Supporting Tables 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.

2.1 Communications with the TOE

8 Mobile VoIP applications communicate with the SIP Server as well as other mobile VoIP application clients, over internet protocol (IP). The endpoints of the communication can be both geographically and logically distant from the TOE, and pass through a variety of other systems. These intermediate systems may be under the control of an adversary, and offer an opportunity for communications with the TOE to be compromised. Although a VPN tunnel provides an outer layer of security for the TOE to communicate with the Enterprise, additional inner layers of security are needed to protect call control traffic (TLS tunnel) and Real Time Services media streams (SRTP tunnel).

9 Plaintext communication with the TOE may allow critical data (such as passwords, keys, configuration settings, and certificates) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE. Several protocols can be used to provide protection; however, each of these protocols has many options that can be implemented and still have the overall protocol implementation remain compliant to the protocol specification listed in the RFC. 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, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises.

10 Even though the communication path is protected, there is a possibility that the external user (be it a SIP server, or another VoIP application) could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the external user as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate remote entity when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing VoIP traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.

[T.UNAUTHORIZED_ACCESS]

2.2 Malicious "Updates"

11 Since a common attack vector used involves attacking unpatched versions of software containing well-known flaws, updating the VoIP application is necessary to ensure that changes to the threat environment are addressed. While the actual update functionality will be implemented in the Enterprise, it is important that the Enterprise be able to accurately determine whether the TOE needs to be updated so that it can be kept current and any inherent vulnerabilities that are discovered can be quickly addressed.

[T.UNAUTHORIZED_UPDATE]

3 SECURITY OBJECTIVES

12 Compliant TOEs will provide security functionality that address threats to the TOE and implements policies that are imposed by law or regulation. The following sections provide a description of this functionality in light of the threats previously discussed that motivate its inclusion in compliant TOEs. The security functionality provided includes protected communications to and between elements of the TOE and the SIP Server and the ability to verify the source of updates to the TOE.

3.1 Protected Communications

13 To address the issues concerning transmitting sensitive data to and from the TOE described in Section 2.1, "Communications with the TOE", compliant TOEs will provide encryption for these communication paths between themselves and the SIP Server. These channels are implemented using TLS for

communication with the SIP Server and SDES-SRTP for communication between endpoints (another VoIP application). TLS and SDES-SRTP are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on TLS and SDES-SRTP to provide interoperability and resistance to cryptographic attack. Whether such additional mechanisms will be evaluated is Scheme-dependent. If such additional mechanisms are not evaluated, guidance must be given to the administrator so that they can be disabled (or shown not to affect the specified security functionality) during TOE operation.

14 In addition to providing protection from disclosure (and detection of modification) for the communications, the TLS protocol described in this document offers two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected. The requirements on the TLS protocol, in addition to the structure of the protocol itself, provide protection against replay attacks such as those described in Section 2.1, usually by including a unique value in each communication so that replay of that communication can be detected.

(FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1, FIA_SIPC_EXT.1,, FCS_SRTP_EXT.1, FCS_TLS_EXT.1, FIA_X509_EXT.1, FTP_ITC.1(*))

3.2 Verifiable Updates

15 As outlined in Section 2.2, “Malicious Updates”, failure by the Enterprise to be able to determine that the TOE needs to be updated could lead to a compromise of the device. Therefore, the TOE is required to be able to provide its current version to the Enterprise through a defined interface.

(FPT_TUD_EXT.1)

4 SECURITY REQUIREMENTS

16 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

17 The CC defines operations on Security Functional Requirements (SFR): 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 **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).

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

4.2 TOE Security Functional Requirements

19 This section identifies the Security Functional Requirements for the TOE. It should be noted that several protocols are used during call establishment: DTLS/TLS, SIP, SDP, and SDES-SRTP. While these protocols (and associated TSS and Testing Assurance Activities) are specified separately, it is expected that a comprehensive description and end-to-end test case/cases can be used to describe and demonstrate the capabilities of the TOE.

20 As indicated above, there is no notion of an "administrator" of the TOE on the device. Administrative settings will be performed either as part of provisioning the device with the TOE or through some function of an MDM capability. In the following requirements, the term "Enterprise" is used to capture this notion of an administrative entity for the TOE.

4.2.1 Cryptographic Support (FCS)

21 In implementing and evaluating the cryptographic functionality of the TOE, it is important to point out that while the production of random keys and salts is required by the TOE, these requirements are contained by reference in the specification of the underlying protocols (TLS, DTLS, and SDES) rather than explicitly through, for example, FCS_CKM.1.

FCS_CKM_EXT.4 Cryptographic key material destruction (Key Material)

FCS_CKM_EXT.4.1 The TSF shall zerioize all plaintext secret and private cryptographic keys and Critical Security Parameters (CSPs) when no longer required.

Application Note:

22 *"CCritical Security Parameters" are defined in FIPS 140-2 as "security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module."*

23 *The zeroization indicated above applies to each intermediate storage area for plaintext key/cryptographic critical security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/cryptographic critical security parameter to another location.*

Assurance Activity:

TSS

24 *The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").*

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 [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:

25 *For the assignment, the ST author should choose the mode or modes in which AES operates. For the first selection, the ST author should choose the key sizes that are supported by this functionality. For the second selection, the ST author should choose the standards that describe the modes specified in the assignment.*

Assurance Activity:

Test

26 *The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.*

FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a ***[selection:***

(1) Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 bits or greater,

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or

(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]

Application Note: As the preferred approach for cryptographic signature, elliptic curves will be required in future publications of this PP.

that meets the following:

Case: Digital Signature Algorithm

- **FIPS PUB 186-3, "Digital Signature Standard"**

Case: RSA Digital Signature Algorithm

- **FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"**

Case: Elliptic Curve Digital Signature Algorithm

- **FIPS PUB 186-3, "Digital Signature Standard"**
- **The TSF shall implement "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard").**

Application Note:

27 *The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.*

28 *While FIPS PUB 186-2 has been revised by FIPS PUB 186-3, it is still allowable to claim conformance to the older standard while products are transitioning to the newer standard. At a future date, products will not be allowed to claim conformance to FIPS PUB 186-2. The ST author makes the selection of the conformance standard as appropriate for the TOE.*

29 *For elliptic curve-based schemes, the key size refers to the log2 of the order of the base point. As the preferred approach for digital signatures, ECDSA will be required in future publications of this PP.*

Assurance Activity:

Test

30 *The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSAVS or DSA2VS), "The Elliptic Curve Digital Signature*

Algorithm Validation System" (ECDSAVS or ECDSA2VS), and "The RSA Validation System" (RSAVS) as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e. FIPS PUB 186-2 or FIPS PUB 186-3). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

FCS_COP.1(3) Cryptographic Operation (Cryptographic Hashing)

FCS_COP.1.1(3) **Refinement:** The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *[selection: SHA-1, SHA-256, SHA-384, SHA-512]* and ~~cryptographic key~~ **message digest** sizes *[selection: 160, 256, 384, 512] bits* that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

Application Note:

31 *The selection of the hashing algorithm must correspond to the selection of the message digest size; for example, if SHA-1 is chosen, then the only valid message digest size selection would be 160 bits.*

Assurance Activity:

Test

32 *The evaluator shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.*

FCS_COP.1(4) Cryptographic Operation (For keyed-hash Message Authentication)

FCS_COP.1.1(4) **Refinement:** The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-[selection: SHA-1, SHA-256, SHA-384, SHA-512],* key sizes *[assignment: key size (in bits) used in HMAC],* **and message digest sizes** [**selection: 160, 256, 384, 512**] **bits** that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

Application note:

33 *In future versions of this PP, SHA-1 may be removed as a valid hash algorithm. Developers are encouraged to transition to the other listed hash alogorithms.*

Assurance Activity:

Test

34 *The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS) " as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.*

FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any),

HMAC_DRBG (any), CTR_DRBG (AES) , Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: a software-based noise source; a TSF-hardware-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum number of bits of entropy at least equal to the greatest bit length required by the protocols and functions supported by the TOE.

Application Note:

35 *It is important to note that FCS_RBG_EXT.1 requires that all RBG operations done by the TSF are done by the portion of the TSF that implements this requirement. This means that the creation of all random key material for the TLS and SDES-SRTP connections must be performed by the TSF.*

36 *NIST Special Pub 800-90, Appendix C describes the minimum entropy measurement that will probably be required in future versions of FIPS-140. If possible this should be used immediately and be required in future versions of this PP.*

37 *For the first selection in FCS_RBG_EXT.1.1, the ST author should select the standard to which the RBG services comply (either 800-90 or 140-2 Annex C).*

38 *SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.*

39 *For the second selection in FCS_RBG_EXT.1.1, the ST author indicates whether the sources of entropy are software-based, hardware-based, or both. If there are multiple sources of entropy, the ST will elaborate each entropy sources and whether it is hardware- or software-based. Hardware-based noise sources are preferred.*

40 *Note that for FIPS Pub 140-2 Annex C, currently only the method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithm, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG.*

41 *The ST author also ensures that any underlying functions are included in the baseline requirements for the TOE.*

Assurance Activity:

TSS

42 *Documentation shall be produced – and the evaluator shall perform the activities – in accordance with Annex D, Entropy and Documentation and Assessment.*

Test

43 *The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.*

Implementations Conforming to FIPS 140-2, Annex C

44 *The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluator shall conduct the following two tests. Note that the "expected values" are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme.*

45 *The evaluator shall perform a Variable Seed Test. The evaluator shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluator shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluator ensure that the values returned by the TSF match the expected values.*

46 *The evaluator shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluator shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluator then invoke the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The evaluator ensure that the 10,000th value produced matches the expected value.*

Implementations Conforming to NIST Special Publication 800-90

47 *The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RBG functionality.*

48 *If the RBG has prediction resistance enabled, each trial consists of (1) instantiate the deterministic RBG (DRBG), (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "Generate one block of random bits" means to generate random bits with the number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).*

49 *If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to re-seed. The final value is additional input to the second generate call.*

50 *The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.*

51 ***Entropy input:** the length of the entropy input value must equal the seed length.*

52 ***Nonce:** If a nonce is supported (CTR_DRBG with no derivation function (df) does not use a nonce), the nonce bit length is one-half the seed length.*

53 ***Personalization string:*** *The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is supported, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*

54 ***Additional input:*** *the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol (SRTP)

FCS_SRTP_EXT.1.1 The TSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2 The TSF shall implement SDES-SRTP supporting the following ciphersuites in accordance with RFC 4568: AES_CM_128_HMAC_SHA1_80.

FCS_SRTP_EXT.1.3 The TSF shall ensure the SRTP NULL algorithm shall be disabled.

FCS_SRTP_EXT.1.4 The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by the Enterprise.

Application Note:

55 *This requirement specifies that the SRTP session that will be used to carry the VIOP traffic will be keyed according to an SDES dialog using the identified ciphersuite. In the future Suite B ciphersuites will be available.*

Assurance Activity:

TSS

56 *The evaluator shall examine the TSS to verify that it describes how the SRTP session is negotiated for both incoming and outgoing calls. This includes how the keying material is established, as well has how requests to use the NULL algorithm or other unallowed ciphersuites are rejected by the TSF.*

Test

57 *The evaluator shall also perform the following test:*

Test 1: The evaluator shall follow the procedure for initializing their device so that they are ready to receive and place calls. The evaluator shall then both place and receive a call and determine that the traffic sent and received by the TOE is encrypted. [1]

[1] While the encryption is provided both by the outer (VPN) and inner (SRTP) tunnels, there is no current requirement to instrument either the TOE or the Enterprise VPN Gateway to demonstrate that SRTP is performing the encryption. Future refinements of this assurance activity may provide more insight into the implementation of this functionality.

FCS_TLS_EXT.1 Transport Level Security

FCS_TLS_EXT.1.1 The TSF shall implement the TLS 1.2 protocol (RFC 5246) compliant with Suite B Profile for TLS (RFC 6460) using mutual authentication with certificates and ciphersuites:

Mandatory Ciphersuites:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 using the 256-bit prime modulus elliptic curve specified in FIPS-186-2;

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using the 384-bit prime modulus elliptic curve specified in FIPS-186-2;

Optional Ciphersuites:

[selection:
None;
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA using the 256-bit prime modulus elliptic curve specified in FIPS-186-2;
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA using the 384-bit prime modulus elliptic curve specified in FIPS-186-2;

Application Note:

58 *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.*

59 *The Mandatory Suite B algorithms (RFC 6460) listed above are the preferred algorithms for implementation. In addition, future publications of this PP will require that the TOE offer a means to deny all connection attempts using specified older versions of the SSL/TLS protocol.*

Assurance Activity:

TSS

60 *The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.*

Test

61 *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).

4.2.2 Identification and Authentication (FIA)

FIA_SIPC_EXT.1 Session Initiation Protocol (SIP) Client

FIA_SIPC_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_SIPC_EXT.1.2 The TSF shall require the user to enter a password to support the use of password authentication for SIP REGISTER function requests as specified in section 22 of RFC 3261.

FIA_SIPC_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]}.

FIA_SIPC_EXT.1.4 Password entered by the user as per FIA_SIPC_EXT.1.2 shall be cleared by the TSF once the TSF is notified that the REGISTER request was successful.

Application Note:

62 *The only SIP request that is required to be authenticated (by the SIP Server) is the REGISTER request; the TOE supports this by providing a user-entered password. While the SIP Server will perform the enforcement and only register the user upon the presentation of the correct password, the client 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_SIPC_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), and to prompt the user for the password when it sends the REGISTER request.*

63 *The intent of the FIA_SIPC_EXT.1.4 element is that the password used for SIP registration are not maintained on the device, and must be re-entered by the user if an additional REGISTER function needs to be sent.*

Assurance Activity:

TSS

64 *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 entered by the user until the time it is cleared by the TSF.*

Test

65 *The evaluator shall also perform the following test:*

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). While it is acceptable for the TSF itself to store and protect these certificates, it is also allowable for the Mobile OS to provide these storage and protection functions. If the TSF provides these functions, then the FIA_X509_EXT.1.Y element shall be included in the body of the ST in this component.

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.

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:

Test

66 *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).

4.2.3 Protection of the TSF (FPT)

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide the Enterpise the ability to query the current version of the TOE software.

Application Note:

67 *Any update of the TOE will be handled by a function of the Mobile OS and is not a function of the TOE itself. However, the TOE must have the ability to correctly report its version to the Mobile OS in order to facilitate decisions on whether to perform the update.*

Assurance Activity:

TSS

68 *The evaluator shall check the TSS to determine that it describes the method by which the TOE reports its current version.*

Guidance

69 *The TOE guidance shall contain the invocation sequence necessary to obtain the current version of the TOE.*

Test

70 *The evaluator shall perform the following test:*

Test 1: The evaluator shall invoke Enterprise functionality to query the current version of the TOE. The evaluator shall confirm that the current version of the TOE is returned.

4.2.4 Trusted Path/Channel (FTP)

FTP_ITC.1(1) Inter-TSF Trusted Channel (SDES-SRTP)

FTP_ITC.1.1(1) **Refinement:** The TSF shall provide a communication channel between itself and a **remote VoIP application using SDES-SRTP as specified in FCS_SRTP_EXT.1** that is logically distinct from other ommunication channels and provides assured identification of its end points and protection of the channel data from modification **and** disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TOE or the remote VoIP application to initiate communication via the trusted channel

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [all communications between the two devices].

Application Note:

71 *This requirement addresses the case where the communications is established between a VoIP Application on another device and the TOE.*

***Assurance Activity**:*

TSS

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

Test

73 *The evaluator shall verify that communication can be initiated from both the TSF and the remote VoIP Application.*

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 Server 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 to initiate communication via the trusted channel

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

Application Note:

74 *The TOE will establish a connection with the SIP server on start-up, and this will persist as long as the device 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

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

76 ***Test***

77 *Testing for this requirement is performed by activities in FTP_ITC.1(1) and FCS_TLS_EXT.1 (and FCS_DTLS_EXT.1 where that component is implemented by the TSF).*

4.3 Security Assurance Requirements

78 The Security Objectives for the TOE in Section 3 were constructed to address threats identified in Section 2. The Security Functional Requirements (SFRs) in Section 4.2 are a formal instantiation of the Security Objectives. The PP draws the Security Assurance Requirements (SARs) from EAL1 to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

79 While this section contains the complete set of SARs from the CC, the Assurance Activities to be performed by an evaluator are detailed both in Section 4.2 as well as in this section.

80 The general model for evaluation of TOEs against STs written to conform to this PP is as follows:

81 After the ST has been approved for evaluation, the Common Criteria Testing Laboratory (CCTL) will obtain the TOE, supporting environmental IT, and the administrative guides for the TOE. The Assurance Activities listed in the ST (which will be refined by the CCTL to be TOE-specific, either within the ST or in a separate document) will then be performed by the CCTL. The CCTL is also expected to perform all of the actions mandated by the Common Evaluation Methodology (CEM) for EAL1. The results of these activities will be documented and presented (along with the administrative guidance used) for validation.

82 For each family, "Developer Notes" are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities (to those already contained in Section 4.2 and the CEM for EAL1) are described as a whole for the family, rather than for each element. Additionally, the assurance activities described in this section are complementary to those specified in Section 4.2.

83 The TOE security assurance requirements, summarized in Table 1, identify the management and evaluative activities required to address the threats identified in Section 2 of this PP.

Table 1: TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance

Assurance Class	Assurance Components	Assurance Components Description
Tests	ATE_IND.1	Independent Testing - Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage

4.3.1 Class ADV: Development

84 At EAL1, the TOE information is contained in the TOE Summary Specification (TSS) portion of the ST guidance as well as documentation available to the end user. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 4.2 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

4.3.1.1 ADV_FSP.1 Basic functional specification

85 The functional specification describes the TOE Security Functionality Interfaces (TSFIs). At EAL1, it is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users, there is little point specifying that such interfaces be described since only indirect testing of such interfaces may be possible. For this PP, the activities for this family should focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional "functional specification" documentation is necessary to satisfy the assurance activities specified.

86 The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Developer Note: As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPR and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section. Since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is

implicitly already done and no additional documentation is necessary.

Content and presentation elements:

ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_ FSP.1.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.
ADV_ FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Assurance Activity:

87 *There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.2, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.*

4.3.2 Class AGD: Guidance Documents

88 The guidance documents will be provided with the developer's security target. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an authorized user.

89 Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger operational environment.

90 Guidance pertaining to particular security functionality is also provided; specific requirements on such guidance are contained in the assurance activities specified in Section 4.2.

4.3.2.1 AGD_OPE.1 Operational User Guidance

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Developer Note: Rather than repeat information here, the developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe what the authorized user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for the authorized user, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for the authorized user, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for the authorized user, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for the authorized user, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

91 *Some of the contents of the operational guidance will be verified by the assurance activities in Section 4.2 and evaluation of the TOE according to the CEM. The following additional information is also required.*

92 *The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.*

93 *The operational guidance shall contain instructions for specifying the ports used for SRTP.*

4.3.2.2 AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator *shall apply* the preparative procedures to confirm that the TOE can be prepared securely for operation.

Assurance Activity:

94 *As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements.*

4.3.3 Class ATE: Tests

95 Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

4.3.3.1 ATE_IND.1 Independent testing - Conformance

96 Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 4.2 are being met, although some additional testing is specified for SARs in Section 4.3. The Assurance Activities identify the additional testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

Assurance Activity:

97 *The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.*

98 *The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to*

merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

99 *The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (SDES, TLS, DTLS).*

100 *The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.*

4.3.4 Class AVA: Vulnerability assessment

101 For the first generation of this protection profile, the evaluation lab is expected to survey open sources to learn what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

4.3.4.1 AVA_VAN.1 Vulnerability survey

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E The evaluator *shall perform* a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E The evaluator *shall conduct* penetration testing, based on the

identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Assurance Activity:

102 *As with ATE_IND the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in Mobility {*mobility component*} in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.*

4.3.5 Class ALC: Life-cycle support

103 At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

4.3.5.1 ALC_CMC.1 Labeling of the TOE

104 This component is targeted at identifying the TOE such that it can be distinguished from other products or version from the same vendor and can be easily specified when being procured by an end user.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements:

ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

105 *The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.*

4.3.5.2 ALC_CMS.1 TOE CM coverage

106 Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

ALC_CMS.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activity:

107 *The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.*

RATIONALE

108 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

109 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

110 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.

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

Table 2: TOE Assumptions

Assumption Name	Assumption Name
A.AUTHORIZED_USER	The cell phone user will follow all provided user guidance. An authorized user is not considered hostile or malicious.
A.AVAILABILITY	Network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.
A.OPER_ENV	The operational environment of the TOE appropriately addresses those requirements, threats, and policies not applicable to the TOE itself, but that are necessary to support the correct operation of the TOE.
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 ST authors when including the requirements described in this document. Modifications, omissions, and additions to the requirements may impact this list, so the ST author should modify or delete these threats as appropriate.

Table 3: Threats

Threat	Description of Threat
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	An update may be needed to a specific version of the TOE, but that specific version may not be known to the Enterprise (that is performing in the update).

Security Objectives for the TOE

Table 4: Security Objectives for the TOE

Objective	Objective Description
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels with authorized IT entities (SIP Server and other VoIP applications).
O.TRUSTED_UPDATES	The TOE will provide the capability to report its current version.

112 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 5: Security Objectives for the Operational Environment

Objective	Objective Description
OE.AUTHORIZED_USER	The cell phone user of the TOE is non-hostile and follows all user guidance.
OE.AVAILABILITY	Network resources will be available to allow VoIP clients to satisfy mission requirements and to transmit information
OE.OPER_ENV	The operational environment will provide a SIP infrastructure to establish a VoIP connection; a PKI to provide certificates; and an execution domain to support correct operation of the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.VERIFIABLE_UPDATES	The Enterprise will provide the capability to update the TOE after that it has determine such an update is necessary.

ANNEX B: NIST SP 800-53/CNSS 1253 MAPPING

113 Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

Application Note:

114 *In this version, only a simple mapping is provided. In future versions, additional narrative will be included that will provide further information for the certification team. This additional information will include details regarding the SFR to control mapping discussing what degree of compliance is provided by the TOE (e.g., fully satisfies the control, partially satisfies the control). In addition, a comprehensive review of the specified assurance activities, and those evaluation activities that occur as part of satisfying the SARs will be summarized to provide the certification team information regarding how compliance was determined (e.g., document review, vendor assertion, degree of testing/verification). This information will indicate to the certification team what, if any, additional activities they need to perform to determine the degree of compliance to specified controls.*

115 *Since the ST will make choices as far as selections, and will be filling in assignments, a final story cannot necessarily be made until the ST is complete and evaluated. Therefore, this information should be included in the ST in addition to the PP. Additionally, there may be some necessary interpretation (e.g.,"modification") to the activities performed by the evaluator based on a specific implementation. The scheme could have the oversight personnel (e.g., Validators) fill in this type of information, or could have this done by the evaluator as part of the assurance activities. The verification activities are a critical piece of information that must be provided so the certification team can determine what, if anything, they need to do in addition to the work of the evaluation team.*

Identifier	Name	Applicable SFRs
AC-4	Information Flow Enforcement	FTP_ITC.1(*)
SC-8	Transmission Integrity	FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_TLS_EXT.1.1, FTP_ITC.1(*), FIA_SIPC_EXT.1, FMT_SRTP_EXT.1.1, FCS_DTLS_EXT.1
SC-9	Transmission Confidentiality	FCS_COP.1(1), FCS_SRTP_EXT.1, FIA_SIPC_EXT.1, FTP_ITC.1(*), FCS_TLS_EXT.1, FCS_DTLS_EXT.1
SC-12	Cryptographic Key Establishment and Management	FCS_TLS_EXT.1, FCS_CKM_EXT.4, FCS_RBG_EXT.1, FCS_DTLS_EXT.1
SC-13	Use of Cryptography	FCS_COP.1(*), FIA_X509_EXT.1

ANNEX C: ADDITIONAL REQUIREMENTS

116 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.

117 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

118 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:

119 *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.

C.1.2 X.509

120 The certificates used by the TSF are those for the distant end TLS connection and the user's certificate (and assocaited private key). While it is acceptable for the TSF itself to store and protect these certificates, it is also allowable for the Mobile OS to provide these storage and protection functions. If the TSF provides these functions, then the the following element shall be included in the body of the ST in the FIA_X509_EXT.1 component.

FIA_X509_EXT.1.Y The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

TSS

121 *The evaluator shall ensure the TSS describes all certificate stores implemented that contain certificates used to meet the requirements of this PP. 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.

Annex D: Entropy Documentation and Assessment

The documentation of the entropy source should be detailed enough that, after reading, the evaluator will thoroughly understand the entropy source and why it can be relied upon to provide entropy. This documentation should include multiple detailed sections: design description, entropy justification, operating conditions, and health testing. This documentation is not required to be part of the TSS.

Design Description

Documentation shall include the design of the entropy source as a whole, including the interaction of all entropy source components. It will describe the operation of the entropy source to include how it works, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the random comes from, where it is passed next, any post-processing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged.

This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source exhibiting probabilistic behavior (an explanation of the probability distribution and justification for that distribution given the particular source is one way to describe this). This argument will include a description of the expected entropy rate and explain how you ensure that sufficient entropy is going into the TOE randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.

Operating Conditions

Documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. It will clearly describe the measures that have been taken in the system design to ensure the entropy source continues to operate under those conditions. Similarly, documentation shall describe the conditions under which the entropy source is known to malfunction or become inconsistent. Methods used to detect failure or degradation of the source shall be included.

Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at startup, continuously, or on-demand), the expected results for each health test,

and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.