# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


TM

# Validation Report

# Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, October 21st, 2013

**Report Number:** CCEVS-VR-PP-0011
**Dated:** 15 April 2015
**Version:** 1.0

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6940**
**Fort George G. Meade, MD 20755-6940**

# ACKNOWLEDGEMENTS

**Common Criteria Testing Laboratory**

***Base and Additional Requirements***
*Gossamer Security Solutions, Inc.*
*Catonsville, Maryland*

# Table of Contents

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4 (IVPNPP14). It presents a summary of the IVPNPP14 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the IVPNPP14 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client. The evaluation was performed by the Gossamer Security Solutions Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2014. This evaluation addressed the base requirements of the IVPNPP14 and the additional requirements contained in Appendix C. Optional requirements defined by Appendix D were not claimed and have not been claimed in subsequent evaluations that claim conformance to the PP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the Gossamer Security Solutions CCTL. Additional review of the PP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the IVPNPP14 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the IVPNPP14, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the IVPNPP14 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the IVPNPP14 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Samsung Galaxy Devices VPN Client, provided by Samsung Electronics Co., Ltd. The evaluation was performed by the Gossamer Security Solutions Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2014.

The IVPNPP14 contains a set of "base" requirements that all conformant STs must include, and in addition, contains both "Selection-based" and "Objective" requirements. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those that that specify security functionality that is desirable but is not explicitly required by the PP. The vendor may choose to include such requirements in the ST and still claim conformance to this PP.

Because these optional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the IVPNPP14 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the IVPNPP14.

| | |
|---|---|
| **Protection Profile** | *Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4* |
| **ST (Base)** | Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client (IVPNCPP14) Security Target, Version 1.1, June 6, 2014 |
| **Evaluation Technical Report (Base)** | Evaluation Technical Report for Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client, Version 1.1, May 23, 2014 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 conformant |
| **CCTL (base)** | Gossamer Security Solutions Inc., Catonsville, MD USA |
| **CCEVS Validators (base)** | Ken Elliott, Aerospace Corporation |
| | Luke Florer, Aerospace Corporation |
| | Meredith Hennan, Aerospace Corporation |
| | Jerry Myers, Aerospace Corporation |
| | Mario Tinto, Aerospace Corporation |

# 3 VPNPP Description

The IVPNPP14 specifies information security requirements for Virtual Private Network (VPN) clients. A VPN provides a protected transmission of private data between VPN Clients and VPN Gateways. The TOE defined by this PP is the VPN Client, a component executing on a remote access client, using a platform API that enables the VPN client application to interact

with other applications and the client device platform (part of the Operational Environment of the TOE). The VPN Client is intended to be located outside or inside of a private network, and provides a secure tunnel to a VPN Gateway. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. All VPN clients that comply with this document will support IPsec.

The focus of the security functionality in the IVPNPP14 is on the following fundamental aspects of a VPN Client:

- Authentication of the VPN Gateway
- Cryptographic protection of data in transit
- Implementation of services

A VPN client can establish VPN connectivity with another VPN endpoint client or a VPN Gateway (that is the "remote" endpoint in the VPN communication). VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity. Authentication of a VPN Gateway is performed as part of the Internet Key Exchange (IKE) negotiation. The IKE negotiation uses a preexisting public key infrastructure for authentication and can optionally use a pre-shared key. When IKE completes, an IPsec tunnel secured with Encapsulating Security Payload (ESP) is established.

It is assumed that the VPN Client is implemented properly and contains no critical design mistakes. The VPN Client relies on the operational environment for its proper execution. The vendor is required to provide configuration guidance (AGD_PRE, AGD_OPE) to correctly install and administer the client machine and the TOE for every operational environment supported.

# 4 Security Problem Description and Objectives

## 4.1 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.

**Table 1: TOE Assumptions**

| Assumption Name | Assumption Definition |
|---|---|
| A.NO_TOE_BYPASS | Information cannot flow onto the network to which the VPN client's host is connected without passing through 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_CONFIG | Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance. |

## 4.2 Threats

**Table 2: Threats**

| Threat Name | Threat Definition |
|---|---|

| Threat Name | Threat Definition |
|---|---|
| T.TSF_CONFIGURATION | Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information. |
| T.TSF_FAILURE | Security mechanisms of the TOE may fail, leading to a compromise of the TSF. |
| T.UNAUTHORIZED_ACCESS | A user may gain unauthorized access to the TOE data. 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 because it is not rendered inaccessible after it is done being used. |

## **4.3** Organizational Security Policies

There are no organizational security policies defined in this PP.

## 4.4 Security Objectives

The following table contains security objectives for the TOE.

**Table 3: Security Objectives for the TOE**

| TOE Security Obj. | TOE Security Objective Definition |
|---|---|
| O.VPN_TUNNEL | The TOE will provide a network communication channel protected by encryption that ensures that the VPN client communicates with an authenticated VPN gateway. |
| 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.TOE_ADMINISTRATION | The TOE will provide mechanisms to allow administrators to be able to configure the TOE. |
| O.TSF_SELF_TEST | The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly. |
| 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. |

The following table contains objectives for the Operational Environment.

**Table 4: Security Objectives for the Operational Environment**

| Environmental Security Obj. | TOE Security Objective Definition |
|---|---|
| OE.NO_TOE_BYPASS | Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE. |
| OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the operational environment. |

| Environmental Security Obj. | TOE Security Objective Definition |
|---|---|
| OE.TRUSTED_CONFIG | Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance. |

# 5 Requirements

As indicated above, requirements in the IVPNPP14 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the Samsung evaluation activity referenced above. Note that many requirements from the PP can be met by either a TOE claiming conformance to the PP or by the underlying platform in that TOE's Operational Environment. SFRs that are shown in **bold** are those that can be met by either a conformant TOE or by the TOE's underlying platform.

| Requirement Class | Requirement Component |
|---|---|
| **FCS: Cryptographic Support** | **FCS_CKM.1(1): Cryptographic Key Generation (Asymmetric Keys)** |
| | **FCS_CKM.1(2): Cryptographic Key Generation (for asymmetric keys - IKE)** |
| | **FCS_CKM_EXT.2: Cryptographic Key Storage** |
| | **FCS_CKM_EXT.4: Cryptographic Key Zeroization** |
| | **FCS_COP.1(1): Cryptographic Operation (Data Encryption/Decryption)** |
| | **FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)** |
| | **FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)** |
| | **FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)** |
| | **FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications** |
| | **FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)** |
| **FDP: User Data Protection** | **FDP_RIP.2: Full Residual Information Protection** |
| **FIA: Identification and Authentication** | **FIA_X509_EXT.1: X.509 Certificate Verification** |
| | **FIA_X509_EXT.2: X.509 Certificate Use and Management** |
| **FMT: Security Management** | FMT_SMF.1: Specification of Management Functions |
| | **FMT_SMF.1: Specification of Management Functions** |
| **FPT: Protection of the TSF** | **FPT_TST_EXT.1: TSF Self Test** |
| | **FPT_TUD_EXT.1: Trusted Update** |
| **FRU: Resource Utilization** | FRU_RSA.1: Maximum Quotas |
| **FTP: Trusted Path/Channels** | **FTP_ITC.1: Inter-TSF Trusted Channel** |

Also note that there are two separate instances of FMT_SMF.1. Some management functions must be performed by a TOE claiming conformance with this PP but other functions can be satisfied by the TOE, its underlying platform, or a VPN gateway that it communicates with.

The following table contains the optional requirements contained in Appendix C and D, and an indication of what evaluation those requirements were verified in (from the list in the

*Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

| Requirement Class | Requirement Component | Verified By |
|---|---|---|
| **FAU: Security Audit** | FAU_GEN.1: Audit Data Generation | |
| | FAU_SEL.1: Security Audit Event Selection | |
| **FDP: User Data Protection** | FDP_IFC_EXT.1: Subset Information Flow Control | |
| **FIA: Identification and Authentication** | FIA_PSK_EXT.1: Pre-Shared Key Composition | Samsung Galaxy Devices VPN Client, June 2014 |

# 6 Assurance Requirements

The following are the assurance requirements contained in the IVPNPP14:

| Requirement Class | Requirement Component |
|---|---|
| **ADV: Development** | ADV_FSP.1 Basic Functional Specification |
| **AGD: Guidance documents** | AGD_OPE.1: Operational User Guidance |
| | AGD_PRE.1: Preparative Procedures |
| **ALC: Life-cycle support** | ALC_CMC.1: Labeling of the TOE |
| | ALC_CMS.1: TOE CM Coverage |
| **ATE: Tests** | ATE_IND.1: Independent Testing - Sample |
| **AVA: Vulnerability Assessment** | AVA_VAN.1: Vulnerability Survey |

# 7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

| APE Requirement | Evaluation Verdict |
|---|---|
| **APE_CCL.1** | Pass |
| **APE_ECD.1** | Pass |
| **APE_INT.1** | Pass |
| **APE_OBJ.2** | Pass |
| **APE_REQ.1** | Pass |

# 8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.

- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the VPNPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

# 9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Gossamer Security Solutions, Inc. *Evaluation Technical Report for Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client,* Version 1.1, May 23, 2014.

[7] Samsung Electronics Co., Ltd. *Samsung Galaxy Devices VPN Client Security Target,* Version 1.0, May 23, 2014.

[8] Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, October 21, 2013.