National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Forcepoint Company

10900 Stonelake Blvd.

Third Floor

Austin, TX 78759, USA

Forcepoint Trusted Access Mobile Client

Report Number:	**CCEVS-VR-10780-2017**
Dated:	**June 1, 2017**
Version:	**0.3**

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

Validation Team

Meredith Hennan
Jerome Myers
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Forcepoint Trusted Access Mobile Client solution provided by Forcepoint Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in May 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12).

The Target of Evaluation (TOE) is the Forcepoint Trusted Access Mobile Client 1.1.

The Target of Evaluation (TOE) 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). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Forcepoint Trusted Access Mobile Client (ASPP12) Security Target, version 0.5, May 30, 2017 and analysis performed by the Validation Team.

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) using the Common

Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Forcepoint Trusted Access Mobile Client 1.1 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12)
ST	Forcepoint Trusted Access Mobile Client Security Target, version 0.5, May 30, 2017
Evaluation Technical Report	Evaluation Technical Report for Forcepoint Trusted Access Mobile Client , version 0.2, May 31, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forcepoint Company
Developer	Forcepoint Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Meredith Hennan Jerome Myers The Aerospace Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is an application installed onto a physical mobile device from the Google Playstore or Apple App Store. The Target of Evaluation (TOE) is the Forcepoint Trusted Access Mobile (TAM) Client.

The TOE is the Trusted Access Mobile Client application for Android and iOS platforms. The TOE is a thin client providing access to a Forcepoint Virtual Mobile Infrastructure (VMI) server from a mobile device. The TOE runs on evaluated Samsung Galaxy S7, S7 Edge, S6, S6 Edge, Note 4, Note 5, Note Edge and Tab S2 devices running Android 6.0.1. The TOE also runs on evaluated Apple iOS 9.3.2 on iPhone and iPad devices using the A7 or A8 processor.

3.1 TOE Evaluated Platforms

The evaluated software version is Version 1.1. The TOE a thin client providing access to a Forcepoint Virtual Mobile Infrastructure (VMI) server from a mobile device. The TOE runs on evaluated Samsung Galaxy S7, S7 Edge, S6, S6 Edge, Note 4, Note 5, Note Edge and Tab S2 devices running Android 6.0.1. The TOE also runs on evaluated Apple iOS 9.3.2 on iPhone and iPad devices using the A7 or A8 processor.

3.2 TOE Architecture

The TOE is an application installed onto a physical mobile device from the Google Playstore or Apple App Store.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device on which the TOE resides.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security Management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

4.1 Cryptographic support

The TAM client also utilizes platform APIs to provide secure network communication using the HTTPS and TLS protocols.

4.2 User data protection

The TAM client does not store sensitive data in local files. The TAM client can access most physical resources on the mobile device, but none of the logical data repositories.

4.3 Identification and authentication

The TAM client utilizes platform provided functionality to verify certificates authenticating network endpoints. The iOS platform support Online Certificate Status Protocol (OCSP) while the Android platform supports both OSCP and Certificate Revocation List (CRL).

4.4 Security management

The TAM client does not include any predefined or default credentials, and utilize the platform recommended storage process for configuration options.

4.5 Privacy

The TAM client does not collect any Personally Identifiable Information (PII) and does not transmit any PII over a network.

4.6 Protection of the TSF

The TAM client relies on the physical boundary of the evaluated platform as well as the Android and iOS operating system for the protection of the TOE’s application components. The TAM client also makes use of specific 3rd party libraries to support WebRTC. All compiled TAM client code is designed to utilize compiler provided anti-exploitation capabilities. The TAM client application is available through the Google Playstore and the Apple store.

4.7 Trusted path/channels

The TAM client utilizes platform API to establish HTTPS and TLS connections to a TAM server.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12)

That information has not been reproduced here and the ASPP12 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP12 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Application Software Protection Profile and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP12 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Forcepoint^{TM} Trusted Access Mobile User's Guide, May 12, 2017

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report for Virtual Mobile Platform Client and Trusted Access Mobile Client, Version 0.2, May 31, 2017 (DTR), and summarized in the Assurance Activity Report (ASPP12) for Trusted Access Mobile Client, Version 0.2, May 31, 2017 (AAR), which is publically available.

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the ASPP12 including the tests associated with optional requirements.

The following depicts a diagram of the test environment used by the evaluators:

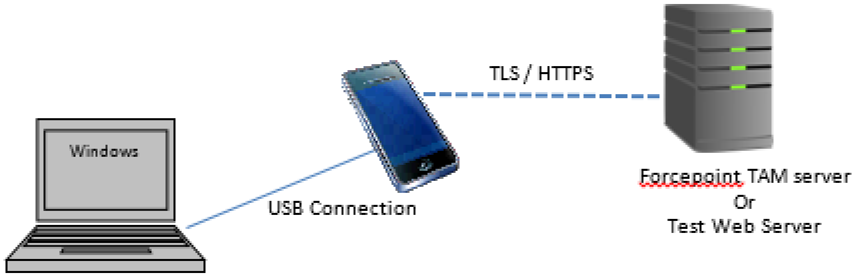

Figure 1: Forcepoint TAM Client TOE Test Environment Setup

9 Evaluated Configuration

The evaluated software version is Version 1.1. The TOE a thin client providing access to a Forcepoint Virtual Mobile Infrastructure (VMI) server from a mobile device. The TOE runs on evaluated Samsung Galaxy S7, S7 Edge, S6, S6 Edge, Note 4, Note 5, Note Edge and Tab S2 devices running Android 6.0.1. The TOE also runs on evaluated Apple iOS 9.3.2 on iPhone and iPad devices using the A7 or A8 processor.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Trusted Access Mobile Client TOE to be Part 2 extended, and to meet the SARs contained in the ASPP12.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Forcepoint Trusted Access Mobile Client 1.1 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the ASPP12 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the ASPP12 and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Forcepoint”, “Raytheon”, “Trusted Access Mobile”, and “Trusted Access”.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

All validator comments have been addressed in the Assumptions and Clarifications of Scope sections.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Forcepoint Trusted Access Mobile Client (ASPP12) Security Target, Version 0.5, May 30, 2017*.

14 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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **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.

15 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12)

[5] Forcepoint Trusted Access Mobile Client (ASPP12) Security Target, Version 0.5, May 30, 2017 (ST)

[6] Assurance Activity Report (ASPP12) for Trusted Access Mobile Client, Version 0.2, May 31, 2017 (AAR)

[7] Detailed Test Report for Virtual Mobile Platform Client and Trusted Access Mobile Client, Version 0.2, May 31, 2017 (DTR)

[8] Evaluation Technical Report for Forcepoint Trusted Access Mobile Client, Version 0.2, May 31, 2017 (ETR)