National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Getac Inc.

400 Exchange, Suite 100

Irvine, CA 92602, U.S.A

Getac MX50

Report Number: CCEVS-VR-10756-2017
Dated: April 6, 2017
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

Validation Team

Herbert Ellis
Meredith Hennan
Kenneth Stutterheim

The Aerospace Corporation

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 Getac MX50 mobile device provided by Getac Inc. 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 April 2017. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, summarized in the Assurance Activity Report; 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 defined in the U.S. Government Protection Profile for Mobile Device Fundamentals, Version 2.0 as modified by the applicable NIAP Technical Decisions.

The Target of Evaluation (TOE) is the Getac MX50 and associated TOE guidance documentation.

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), as interpreted by the Assurance Activities contained in the MDF Protection Profile. This Validation Report applies only to the specific version of the TOE when configured as directed in the Getac MX50 Administrator Guidance Instructions. 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 presented in the proprietary 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 associated with the Protection Profile 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 presented in the evaluation sensitive Evaluation Technical Report are consistent with the evidence produced.

The technical information included in this report was obtained from the Getac MX50 (MDFPP20) Security Target, Version 1.0, April 5, 2017 as configured using the Getac MX50 Administrator Instructions Version 0.8 April 2, 2017, and the analysis of evaluation evidence 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) work units specific to the technology described by the PP 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 Product Compliant 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	Getac MX50
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014
ST	Getac MX50 Security Target, Version 1.0, April 5, 2017
Evaluation Technical Report	Evaluation Technical Report for Getac MX50 , version 0.3, April 5, 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	Getac Inc.
Developer	Getac Inc.
Common Criteria Testing Lab (CCTL)	Tammy Compton, Raymond Smoley, Gossamer Security Solutions, Inc.

Item	Identifier
CCEVS Validators	Herbert Ellis, Meredith Hennan, Kenneth Stutterheim, The Aerospace Corporation

3 Architectural Information

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

The Target of Evaluation (TOE) is a ruggedized mobile device designed to support military and civil service users. Based upon Android 5.1.1, the TOE provides wireless and wired connectivity out of the box.

Snapbacks can be used to add optional modules (e.g., cellular). The TOE includes a port to attach a snapback module that adds WWAN, USB, USB storage encryption or a second battery.

The evaluated TOE contains either 64GB/128GB of internal Flash storage and either 2GB/4GB of memory.

The TOE is the Getac Inc. MX50, a ruggedized tablet featuring a 5.7" (1280x720 HD) display; an Intel Z8350 1.44 GHz x86 CPU; micro USB; Gleanair and AB Military connector; microSD; 14-pin modular connector; WiFi/Bluetooth radio. The TOE runs Android 5.1.1.

The MX50 does not have a cellular chip for mobile broadband. The MX50 only has a WiFi/Bluetooth chip and Ethernet (via military connector or USB-to-Ethernet) for networking (connecting to WiFi or Bluetooth networks).

3.1 TOE Evaluated Platforms

The evaluated configuration consists of a Getac MX50 running on Android 5.1.1.

3.2 TOE Architecture

The TOE provides an Application Programming Interface to mobile applications and provides users installing an application the option to either approve or reject an application based upon the API access that the application requires.

The TOE provides users with the ability to protect Data-At-Rest with AES encryption, including all user and mobile application data stored in the user's data partition. The TOE affords protection to all user and application cryptographic keys stored in the TOE. Moreover, the TOE provides users the ability to AES encrypt data and files stored on an SD Card inserted into the device.

The TOE can interact with Mobile Device Management solutions to allow enterprise control of the configuration and operation of the device to ensure adherence to enterprise-wide policies.

The TOE protects itself from tampering and bypass by offering a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In each case the TOE implements a set of policies to control the services available and to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE's physical boundary is the physical perimeter of its enclosure (without the rear access cover present, so that one can access and replace the device's battery).

4 Security Policy

This section summaries the security functionality provided by the Getac MX50:

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

4.1 Cryptographic support

The TOE includes cryptographic modules with CAVP validated algorithms used for cryptographic functions such as: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS and HTTPS and to encrypt the media (including the generation and protection of data, right, and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

4.2 User data protection

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected.

4.3 Identification and authentication

The TOE supports features related to identification and authentication. From a user perspective, a password (i.e., Password Authentication Factor) must be correctly entered to

unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display. The TOE limits the frequency of password entry and when a configured number of failures occurs, the TOE takes an appropriate action such as performing a full wipe of protected content or some other administrator-defined action. Passwords can be constructed using upper and lower case characters, numbers, and special characters. Passwords up to 14 characters in length are supported.

The TOE can serve as an IEEE 802.1X supplicant and to use X509v3 certificates and perform certificate validation for a number of functions when applicable such as EAP-TLS, TLS, and HTTPS exchanges.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions claimed in the corresponding Security Target (and conforming to the MDFPP requirements) as well as other functions commonly found in mobile devices. Some of the available functions are available only to the mobile device users while others may be restricted to administrators operating through a Mobile Device Management solution if the TOE has been enrolled. If the TOE has been enrolled in a Mobile Device Management solution and is subsequently un-enrolled, the TOE will perform a full wipe of protected data to complete the un-enrollment.

4.5 Protection of the TSF

The TOE implements features to ensure the reliability and integrity of its security features. It protects data such as cryptographic keys so that they are not accessible or exportable. It provides a timing mechanism to ensure that reliable time information is available (e.g., for cryptographic operations and perhaps user accountability). It enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. The TOE includes the capability to protect itself from modification by applications as well as to isolate the address spaces of applications from one another to protect those applications.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any self-test fails, the TOE will not go into an operational mode. It also includes a mechanism (i.e., verification of the digital signature of each new image) so that the TOE can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

4.6 TOE access

The TOE can be locked, thereby obscuring its display, either by a user or automatically after a configured interval of inactivity. The TOE also has the capability to display an advisory message (banner) when users unlock the TOE for use.

4.7 Trusted path/channels

The TOE supports the use of IEEE 802.11-2012, IEEE 802.1X, and EAP-TLS to secure communications channels between itself and other trusted network devices.

5 Assumptions

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

- Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014

That information has not been reproduced here and the MDFPP20 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 MDFPP20 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Any other functionality provided by the device 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 Mobile Device Fundamentals Protection Profile and performed by the evaluation team).
- This evaluation covers only the specific device model 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 MDFPP 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:

- Getac MX50 Administrator Guidance Instructions, Version 0.8, April 2, 2017

Any additional customer documentation delivered with the product or that is available through download was not included in the scope of the evaluation, and therefore should not be relied upon when configuring or using the products as evaluated.

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 proprietary Detailed Test Report (MDFPP20) for Getac MX50, Version 0.2, April 3, 2017 (DTR) and summarized in the Assurance Activity Report (MDFPP20) for Getac Inc. MX50 Tablet, version 0.3, April 5, 2017, which is publically available.

The following diagrams depict the test environments used by the evaluators.

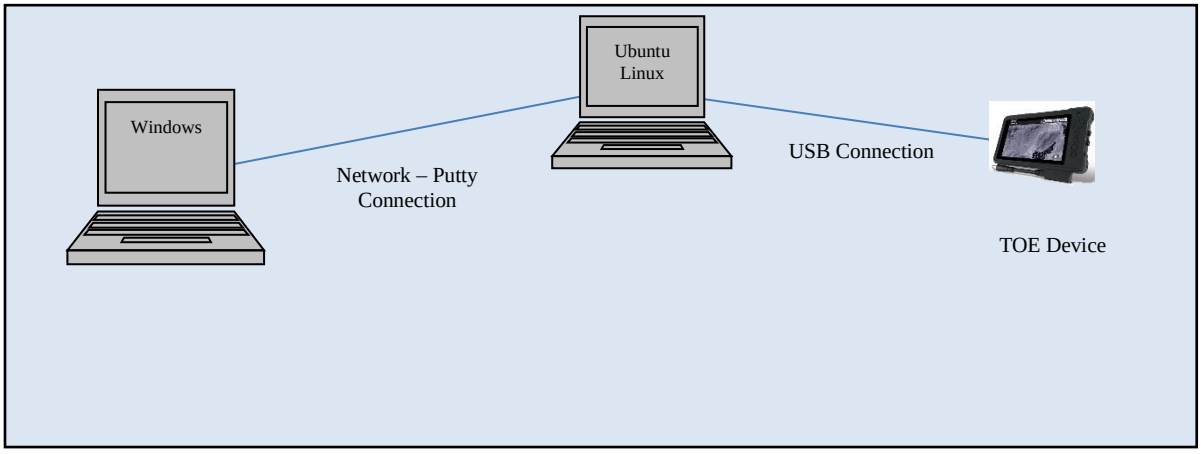

Figure 1 Evaluator Test Setup 1

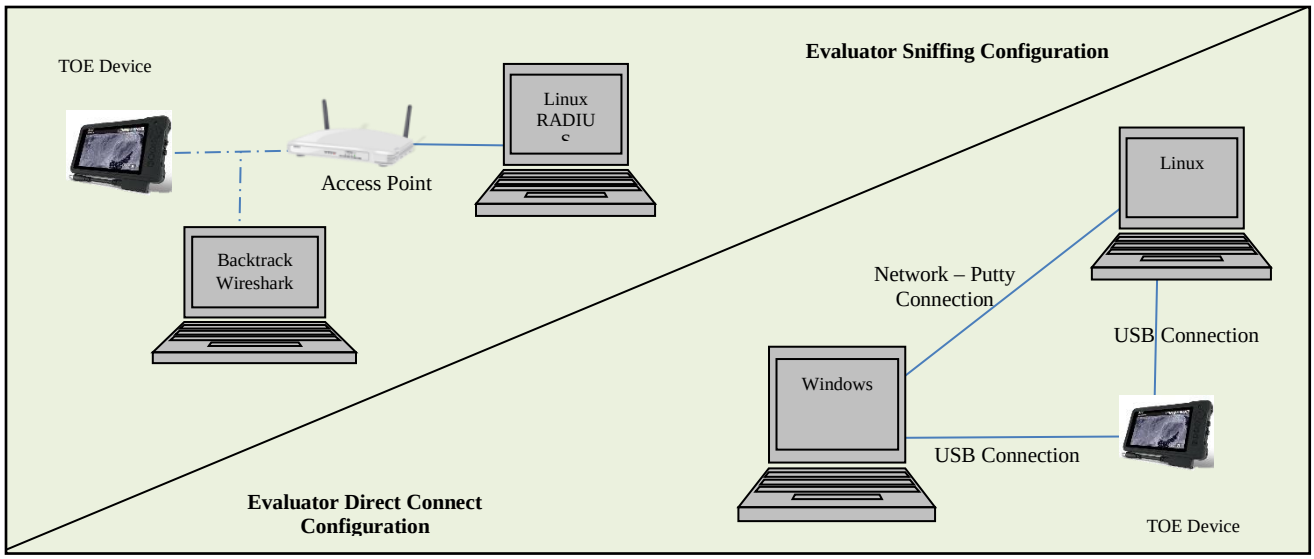

Figure 2 Evaluator Test Setup 2

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 MDFPP20 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of a Getac MX50 running on Android 5.1.1. To use the product in the evaluated configuration, the product must be configured as specified in Getac MX50 Administrator Instructions Version 0.8 April 2, 2017.

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 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 Getac MX50 to be Part 2 extended, and to meet the SARs contained in the MDFPP v2.

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 Getac MX50 product that are consistent with the Common Criteria, and product security function descriptions that supported the requirements.

The validators 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 MDFPP20 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 validators 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 validators 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 MDFPP20 and recorded the results in an evaluation sensitive Test Report, and summarized in the publically available AAR.

The validators 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 includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerabilities. All vulnerabilities have been addressed and are being distributed via the carriers.

The evaluator searched the National Vulnerability Database located at URL: (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database URL: (http://www.kb.cert.org/vuls/) with the following search terms: "Getac", "MX50", "Getac MX50", "Android", and “Openssl".

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

The evaluated configuration of the Getac MX50 did not include the testing of any of the available optional Snapback modules, which are used to add capabilities such as WWAN, USB, USB storage encryption or a second battery; none of those were tested, and no assumptions should be made or inferred regarding their correct operation.
The MX50 does not have a cellular chip for mobile broadband, cellular capability can only be added via a Snapback.
The device requires the use of a compatible Mobile Device Management solution to set the device into its evaluated configuration. The vendor claims that any compatible Mobile Device Management solution can be used, however the only MDM used for testing was the

agent specified in the admin guide. The compatibility of any other MDM solution was not verified through this evaluation, and consumers are solely responsible for ensuring their enterprise solution is compatible.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Getac MX50 (MDFPP20) Security Target, Version 1.0, April 5, 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 Mobile Device Fundamentals, Version 2.0, 17 September 2014

[5] Getac MX50 (MDFPP20) Security Target, Version 1.0, April 5, 2017 (ST)

[6] Assurance Activity Report (MDFPP20) for Getac Inc. MX50 Tablet, Version 0.3, April 5, 2017 (AAR)

[7] Detailed Test Report (MDFPP20) for MX50, Version 0.2, April 3, 2017 (DTR)

[8] Evaluation Technical Report for Getac MX50, Version 0.3, April 5, 2017 (ETR)

[9] Getac MX50 Administrator Guidance Instructions, Version 0.8, April 2, 2017 (AGD)