National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Kyocera Corporation

9520 Towne Centre Drive, Suite 200

San Diego, California 92121

Kyocera DuraForce PRO Mobile Device

Report Number: CCEVS-VR-10742-2017
Dated: January 5, 2017
Version: 0.4

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
Ken Stutterheim
Aerospace Corporation
Columbia, MD

Noel Richards
National Security Agency
Fort Meade, MD

Common Criteria Testing Laboratory

James Arnold
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 Kyocera DuraForce PRO Mobile Device solution provided by Kyocera Corporation. 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 January 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 Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is the Kyocera DuraForce PRO Mobile Device 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). 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 Kyocera DuraForce PRO Mobile Device Security Target, version 1.0, January 5, 2017.

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 National Voluntary Laboratory Assessment Program (NVLAP) commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities which are the interpretations of the

Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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:	Kyocera DuraForce PRO Mobile Device (Specific models identified in Section 3.1)
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014
ST:	Kyocera DuraForce PRO Mobile Device Security Target, version 1.0, January 5, 2017
Evaluation Technical Report	Evaluation Technical Report for Kyocera DuraForce PRO Mobile Device , version 0.3, January 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	Kyocera Corporation
Developer	Kyocera Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Herbert Ellis Meredith Hennan, Ken Stutterheim, Noel Richards

Item	Identifier

3 Architectural Information

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

The Target of Evaluation is the Kyocera DuraForce PRO smartphone which includes the Qualcomm MSM8952 processor along with the associated guidance documentation.

The Kyocera DuraForce PRO includes a 5.0 inch, Full HD 1920x1080 resolution LCD display; a 13MP rear facing camera, 5MP front facing camera and a Super Wide View 1080p HD video Action Camera; 2GB of RAM; 32GB of built-in storage; and a microSD card slot. The Kyocera DuraForce PRO can operate on CDMA, GSM, UMTS and LTE communication networks[1].

The Kyocera DuraForce PRO is a mobile device that supports individual users as well as corporate enterprises. The Kyocera DuraForce PRO is based upon Android 6.0.1 as customized by Kyocera.

The TOE provides wireless connectivity and creates a runtime environment for applications designed for the mobile Android environment. The TOE provides telephony features (make and receive phone calls, send and receive SMS messages), and networking features (connect to Wi-Fi networks, send and receive MMS messages, connect to mobile data networks).

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

Model	Model #	Storage	RAM	Kernel Version	Build #	Carrier Variant
DuraForce PRO	E6810	32GB	2GB	3.10.84	77f9a2518fcf54e010ac4708f980bc92	Verizon
DuraForce PRO	E6820	32GB	2GB	3.10.84	5af5d0a4566fec0b8bab756b3386c667	AT&T
DuraForce PRO	E6830	32GB	2GB	3.10.84	c0307913ad6ff1e293bf8a646988d5bd	Sprint

[1] CDMA is available only for Sprint and Verizon variants of the mobile device.

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 (DAR) with AES encryption, which includes 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 use AES to encrypt data and files stored on an SD Card inserted into the device.

Finally, the TOE can interact with a Mobile Device Management 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 only 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 both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

3.3 Physical Boundaries

The TOE's physical boundary is the physical perimeter of the mobile device's enclosure.

4 Security Policy

This section summarizes the security functions provided by DuraForce PRO:

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 two cryptographic modules with CAVP validated algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with 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 also to encrypt the media (to include the generation and protection of data, right, and key encryption keys) which are used by the

TOE. Many of these cryptographic functions are 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 data through the use of encryption so that even if a device is physically lost, the data remains protected.

4.3 Identification and authentication

The TOE supports a number of features related to identification and authentication. From a user perspective, except for limited functions such as making phone calls to an emergency number and receiving notifications, 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 attempts and when a preconfigured number of failures is exceeded, the TOE performs a full wipe of protected content. Passwords up to 14 characters can be supported and can be constructed using upper and lower case characters, numbers, and special characters.

The TOE serves as an IEEE 802.1X supplicant and uses 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 the interfaces necessary to manage the security functions claimed in the corresponding Security Target (and that conform 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 other functions are restricted to administrators operating through a Mobile Device Management solution. If the TOE has been enrolled in a MDM and is subsequently un-enrolled, it issues an alert to the administrator and wipes the device to complete the un-enrollment.

4.5 Protection of the TSF

The TOE implements functions 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 does not enter an operational mode. It also includes a mechanism (i.e., verification of the digital signature of each new image) so that the TOE itself 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 is lockable, thereby obscuring its display, either by a user or after a configured interval of inactivity.

The TOE is able to attempt to connect to wireless networks if so configured.

4.7 Trusted path/channels

The TOE supports the use of IEEE802.11-2012, IEEE802.1X, 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 Protection Profile For Mobile Device Fundamentals, Version 2, 17 September 2014 (MDFPP). That information has not been reproduced here and the MDFPP should be consulted if there is interest in that material.

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 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 MDFPP and any 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:

- Kyocera DuraForce PRO Common Criteria Guidance Manual, version 1.2 dated January 5, 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 Detailed Test Report (MDFPP20) for Kyocera DuraForce PRO Mobile Device, version 0.2, October 27, 2016 (DTR) and summarized in the Assurance Activity Report (MDFPP20) for Kyocera DuraForce PRO Mobile Device, version 0.3, January 5, 2017 (AAR), which is publically available.

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

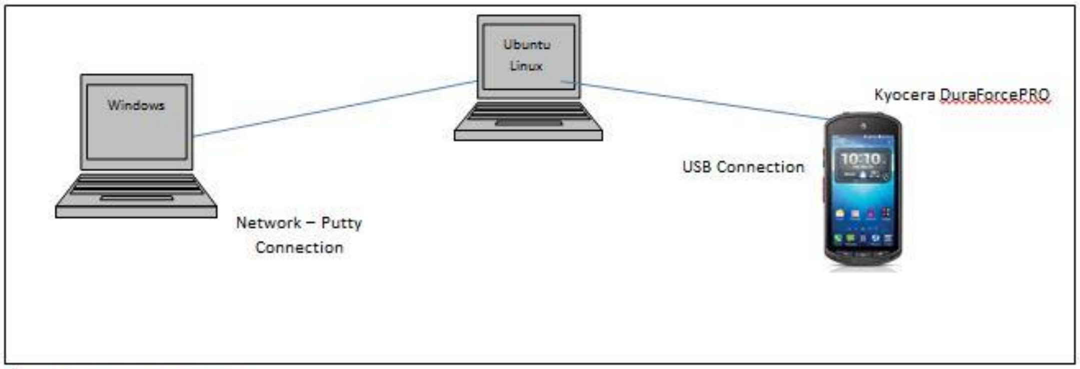

Figure 1 Evaluator Test Setup 1

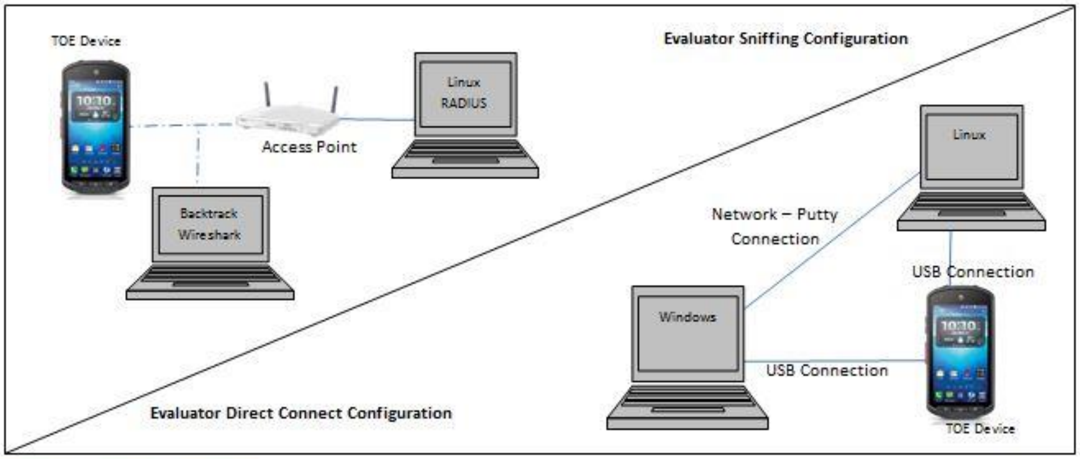

Figure 2 Evaluator Test Setup 2

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 to the Kyocera DuraForce PRO Common Criteria Guidance Manual, version 1.2, January 5, 2017 document and performed the tests specified in the MDFPP20 to include tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of the Kyocera DuraForce PRO devices.

To use the product in the evaluated configuration, the product must be configured as specified in Kyocera DuraForce PRO Common Criteria Guidance Manual, version 1.2, January 5, 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 Kyocera DuraForce PRO devices to be Part 2 extended, and to meet the SARs contained in the MDFPP.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Kyocera DuraForce PRO Mobile Device products that are consistent with the Common Criteria, and product security function descriptions that supported the requirements.

The validation team 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 validation team 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 relevant AGD CEM work unit. The evaluation team ensured the adequacy of the Common Criteria Guidance in describing how to use and or administer the operational TOE. The guide was assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team 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 the relevant ALC CEM work units. The evaluation team found that the TOE was identified.

The validation team 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 relevant ATE CEM work unit. The evaluation team performed the tests specified by the assurance activities in the MDFPP20 and recorded the results in a Test Report, and summarized in the AAR.

The validation team 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 the relevant AVA CEM work units. 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 vulnerabilities. All vulnerabilities have been addressed and are being distributed via the carriers.

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: "Kyocera Explorer", "Kyocera", "Explorer", "Kyocera DuraForce Pro", "DuraForce", "Android", "Android 6", "Openssl".

The validation team 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

References are made throughout the documentation regarding Mobile Device Management Solutions, the consumer is reminded that although the product provides the capability to be managed via a compatible MDM product, that functionality was not tested as part of this evaluation and no claims can be made as to proper operation.

Additionally, the USB update method known as Software Repair Assistant (SRA) is disabled in CC mode, therefore this functionality was not tested as a part of this evaluation and no claims can be made as to proper operation.

The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation does not cover, nor does it endorse, the use of any particular MDM solution and only the MDM interfaces of the products were exercised as part of the evaluation.

Furthermore, to configure CC Mode, users need to obtain CC Mode APK from Kyocera or Kyocera approved point of contacts. The usage of CC Mode application may be governed by additional contracts/agreements regulated by Kyocera International Inc.

The Kyocera CC guide includes password history as part of the CC configuration. Although maintaining password history is good practice, it is not required for CC compliance.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Kyocera DuraForce PRO Mobile Device (MDFPP20) Security Target, Version 1.0, January 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] Kyocera DuraForce PRO Mobile Device (MDFPP20) Security Target, version 1.0, January 5, 2017 (ST)

[6] Assurance Activity Report (MDFPP20) for Kyocera DuraForce PRO Mobile Device, version 0.3, January 5, 2017 (AAR)

[7] Detailed Test Report (MDFPP20) for Kyocera DuraForce PRO Mobile Device, version 0.2, October 27, 2016 (DTR)

[8] Evaluation Technical Report for Kyocera DuraForce PRO Mobile Device, version 0.3, January 5, 2017 (ETR)

[9] Kyocera DuraForce PRO Common Criteria Guidance Manual, version 1.1, November 8, 2016