National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

KeyW Corporation

7880 Milestone Parkway, Suite 300

Hanover, MD 21076 USA

KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1

Report Number: CCEVS-VR-10801-2017
Dated: August 10, 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

Meredith Hennan
Jerome Myers
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 KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1 solution provided by KeyW 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 August 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) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10).

The Target of Evaluation (TOE) is the KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1.

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 KeyW BlackBerry Suite B Data at Rest (ASPP12/ASFEEP10) Security Target, Version 1.0, August 7, 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	KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Application Software, Version 1.2, 22 April 2016 (ASPP12) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)
ST	KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1 Security Target, Version 1.0, August 7, 2017
Evaluation Technical Report	Evaluation Technical Report for KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1, Version 0.3, August 7, 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	United States Special Operations Command (USSOCOM)
Developer	KeyW Corporation

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Meredith Hennan Jerome Myers Aerospace Corporation Columbia, MD

3 Architectural Information

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

The KeyW BlackBerry Suite B Data at Rest application (i.e., the TOE) is a file encryption tool that runs on a BlackBerry 10.3 mobile device. The BlackBerry Advanced Data at Rest Protection (ADARP) relays all operations on files within the BlackBerry work space to the TOE which encrypts or decrypts the file contents automatically. The TOE runs as a BlackBerry required application, meaning the BlackBerry operating system will ensure that the mobile device features are available only when the TOE is running.

The TOE utilizes the BlackBerry 10.3 operating system for storage of passwords, keys and for Deterministic Random Bit Generation (DRBG). However, the TOE implements its own encryption, decryption, and keyed-Hashing functions, which have been certified through CAVP.

The KeyW BlackBerry Suite B Data at Rest TOE is also known as KEYWprotect. The TOE provides an AES-based Data at Rest (DAR) encryption model that is used to encrypt the BlackBerry work space data when BlackBerry 10.3 mobile devices are unlocked including encrypting data received when the BlackBerry work space is locked. The TOE is an application on the BlackBerry 10.3 mobile device.

The TOE utilizes BlackBerry Advanced Data at Rest Protection (ADARP) features to relay all file operations within the BlackBerry work space when the BlackBerry 10.3 mobile device is in the unlocked and locked states. When the BlackBerry 10.3 mobile device is unlocked, all BlackBerry work space data created by other applications is automatically encrypted by the TOE and stored in the BlackBerry work space via the BlackBerry File System (FSYS) Relay API feature. When the BlackBerry 10.3 mobile device is locked, all BlackBerry work space data received by other applications is automatically encrypted by the TOE and stored in the BlackBerry work space via the BlackBerry Data Lock Queue (DLQ) Relay API feature. Encrypted work space data is decrypted as needed only after a user presents valid authentication factors. Therefore, no clear text is ever written to the BlackBerry work space file system.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

Device	Processor
Classic	Qualcomm S4 (MSM8960)
Passport	Qualcomm Snapdragon 801
Leap	Qualcomm S4 (MSM8960)
Z30	Qualcomm S4 (MSM8960)
Q10 Porsche	Qualcomm S4 (MSM8960)
Q10	Qualcomm S4 (MSM8960)
Z10 Porsche	Qualcomm S4 (MSM8960)
Z10	Qualcomm S4 (MSM8960)

3.2 TOE Architecture

KEYWprotect is an application that is installed as a required application when the BlackBerry device is provisioned for use. Being a required application, the BlackBerry 10.3 platform ensures that the TOE is running prior to presenting the home screen to the user, and prevents all actions, which could uninstall the TOE. The TOE provides its own cryptographic functionality, which has been FIPS validated through CAVP certifications.

All attempts to create new files within the BlackBerry work space are relayed to the TOE by Blackberry ADARP and the TOE encrypts these files before they are written to the work space file system. Therefore, no clear text version of the file is ever created on the work space file system.

The TOE generates and stores the following keys and Critical Security Parameters (CSPs) for the File System Relay:

- The TOE generates and stores a 256-bit SALT in the BlackBerry Certificate Manager.
- The TOE derives a 256-bit HASH Key Encryption Key (KEK) from the user's password and 256-bit SALT using PBKDF and stores this KEK in the BlackBerry Certificate Manager.
- The TOE generates and stores a 256-bit Master KEK encrypted by the 256-bit HASH KEK in the BlackBerry Certificate Manager using AES Key Wrap.
- The TOE generates and stores a File Encryption Key (FEK) and a File Authentication Key (FAK) encrypted by the 256-bit Master KEK in the associated metadata of each encrypted file using AES Key Wrap.
- The TOE generates and stores a Message Authentication Code (MAC) immediately following each ciphertext block in each encrypted file.

The TOE generates and stores the following keys and Critical Security Parameters (CSPs) for the Data Lock Queue Relay:

- The TOE generates and stores a static 521-bit ECC DLQ Master encryption keypair in the BlackBerry Certificate Manager.
- The TOE generates and stores the following keys and CSPs for each open/write of a file or after crossing the 1 megabyte Anchor Point boundary, which represents a

starting point position in the file for encrypting data and therefore also the position where data will be decrypted:

- The TOE generates an ephemeral 521-bit ECC Anchor Point keypair.
- The TOE computes a shared secret using ECC CDH Primitive from the 521-bit ECC DLQ Master encryption keypair and ephemeral 521-bit ECC Anchor Point keypair.
- The TOE derives a 256-bit Root Encryption Key (REK) from the shared secret using SHA.
- The TOE derives an ephemeral 521-bit ECC DLQ keypair, static 521-bit ECC Anchor Point keypair, 36-byte Nonce, and a 128-bit IV from the REK using a KBKDF.
  - The TOE stores the 128-bit IV in the Anchor Point context contained in volatile memory.
  - The TOE stores the compressed ephemeral 521-bit ECC Anchor Point in the associated metadata of the Anchor Point.
- The TOE computes a 256-bit MAC key, a 256-bit Key Encryption Key (KEK), a 256-bit Data Encryption Key (DEK), and a 256-bit MAC tag using ECC KAS.
  - The TOE stores the 256-bit KEK in the Anchor Point context contained in volatile memory when processed as the Master Anchor Point context.
  - The TOE stores the 256-bit DEK in the Anchor Point context contained in volatile memory where the DEK is encrypted by a 256-bit Master Anchor Point context KEK for only decrypt operations.
  - The TOE stores the 256-bit MAC key encrypted by the REK using AES Key Wrap, and the 256-bit MAC tag in the associated metadata of the Anchor Point.

- The TOE chains forward the 256-bit DEK and 128-bit IV for each 4 kilobytes of file data using a KBKDF where the DEK is encrypted by a 256-bit Master Anchor Point context KEK for only decrypt operations.
- The TOE stores the chain counter in the Anchor Point context contained in volatile memory.

3.3 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the evaluated device (BlackBerry 10.3) 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. Protection of the TSF
6. Trusted path/channels

4.1 Cryptographic support

The TOE operates on a BlackBerry 10.3 mobile device and uses features provided by the platform for key storage, user credential storage, and Deterministic Random Bit Generation (DRBG). The TOE implements its own algorithms for AES, Key Wrapping, key-based and password-based Key Derivation, Key Establishment, cryptographic hashing and keyed-hashing.

4.2 User data protection

The TOE protects user data by providing an integrated file encryption and file data authentication capability that automatically encrypts new files and decrypts files upon user demand. The TOE utilizes 256-bit AES encryption for confidentiality and HMAC-SHA-384 for file data integrity.

4.3 Identification and authentication

The TOE authenticates a user by requiring a password before any file data decryption operation is initiated. Without the correct password, the user is unable to decrypt the keys necessary to obtain clear text data from the BlackBerry work space file system.

4.4 Security management

The TOE supports encryption while in the locked state, but does not allow decryption or integrity operations until the user authenticates to the device upon first use of the TOE. The TOE allows the user to change their password for management purposes.

4.5 Protection of the TSF

The TOE relies on the physical boundary of the evaluated platform as well as the BlackBerry 10.3 operating system for the protection of the TOE's application components.

Updates to the TOE are handled by the BlackBerry Enterprise Services (BES) management software.

4.6 Trusted path/channels

The TOE does not transmit any data between itself and another network entity. All of the data managed by the TOE resides on the evaluated platform (BlackBerry 10.3).

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) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)

That information has not been reproduced here and the ASPP12/ASFEEP10 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/ASFEEP10 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 with File Encryption Extended Package 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/ASFEEP10 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:

- KeyW BB10 Suite B Data at Rest v1.2.2.1 User Guide, Version 1.1, July 21, 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 (ASPP12/ASFEEP10) for KeyW BlackBerry Suite B Data at Rest, Version 0.3, August 7, 2017 (DTR).

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/ASFEEP10 including the tests associated with optional requirements.

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

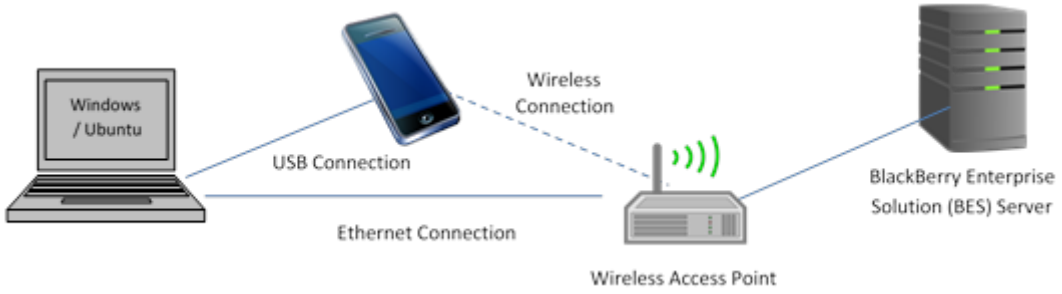

Figure 1: Test Setup

9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Device	Processor
Classic	Qualcomm S4 (MSM8960)
Passport	Qualcomm Snapdragon 801
Leap	Qualcomm S4 (MSM8960)
Z30	Qualcomm S4 (MSM8960)
Q10 Porsche	Qualcomm S4 (MSM8960)
Q10	Qualcomm S4 (MSM8960)
Z10 Porsche	Qualcomm S4 (MSM8960)

Z10	Qualcomm S4 (MSM8960)

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 BlackBerry Suite B Data at Rest, Version 1.2.2.1 TOE to be Part 2 extended, and to meet the SARs contained in the ASPP12/ASFEEP10.

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 KeyW BlackBerry Suite B Data at Rest, Version 1.2.2.1 products 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/ASFEEP10 related to the examination of the information contained in the TOE Summary Specification (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/ASFEEP10 and recorded the results in a proprietary Test Report, and summarized in the AAR, which is publically available.

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: “KeyW, KeyWProtect, KeyW Protect, BlackBerry, and BES”.

Additionally, the evaluator ran a virus scanner against the TOE’s files and did not find any viruses.

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: *KeyW BlackBerry Suite B Data at Rest (ASPP12/ASFEEP10) Security Target, Version 1.0, August 7, 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) and Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System, Version 1.0, 10 November 2014 (ASFEEP10)

[5] KeyW BlackBerry Suite B Data at Rest (ASPP12/ASFEEP10) Security Target, Version 1.0, August 7, 2017 (ST)

[6] Assurance Activity Report (ASPP12/ASFEEP10) for BlackBerry Suite B Data at Rest, Version 0.3, August 7, 2017 (AAR)

[7] Detailed Test Report (ASPP12/ASFEEP10) for BlackBerry Suite B Data at Rest, Version 0.3, August 7, 2017 (DTR)

[8] Evaluation Technical Report for KeyW BlackBerry Suite B Data at Rest, Version 0.3, August 7, 2017 (ETR)