National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

BlackBerry Unified Endpoint Management (UEM) Server and Android Client, version 12

Report Number: CCEVS-VR-11040-2020
Dated: 28 April 2020
Version: 0.1

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

Lisa Mitchell
Clare Olin
Sheldon Durrant
Chris Thorpe

Common Criteria Testing Laboratory

Cornelius Haley
Raymond Smoley
Bright Sun
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 BlackBerry Unified Endpoint Management (UEM) Server and Android Client version 12 solution provided by BlackBerry, LTD. 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 2020. 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 EAL 1.

The Target of Evaluation (TOE) is the BlackBerry Unified Endpoint Management (UEM) Server and Android Client version 12.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the BlackBerry UEM Server and Android Client Version (MDMPP40/MDMA10/PKGTLS11) Security Target, Version 0.6, 28 April 2020 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) for Evaluation Assurance Level (EAL) 1 through 4 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	BlackBerry UEM Server and Android Client version 12 (Specific models identified in Section 3.1)
Protection Profile	PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 2020-01-27 The PP-Configuration is comprised of the following: • Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 with the following packages: ○ Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March • PP-Module for MDM Agents, Version 1.0, 2019-04-25
ST	BlackBerry UEM Server and Android Client Version (MDMPP40/MDMA10/PKGTLS11) Security Target, Version 0.6, 28 April 2020
Evaluation Technical Report	Evaluation Technical Report for BlackBerry UEM Server and Android Client Version 12, ETR Version 0.3, 28 April 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	BlackBerry, LTD

Item	Identifier
Developer	BlackBerry, LTD
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	

3 Architectural Information

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

The UEM Server provides centralized management of mobile devices and the UEM Android Client Agent (installed on each android device) enforces the policies of the Server on each android device.

The BlackBerry UEM server, including the Core and UI security enforcing components, is implemented with a combination of Java and native code running on Windows Server 2016 with Java JRE 8.0. The UEM Server consists of a number of components. However, only the Core and UI components are included in the TOE for the purpose of evaluation. The other components are either disabled or play no role in any security enforcement.

The UEM Server requires a SQL database to operate and can optionally be configured to utilize an LDAP server for user authentication as well as a SYSLOG server to export audit records. Some other components such as Exchange are not included in the scope of evaluation or are not security relevant – the BBR (Blackberry router) and BlackBerry NOC are network routing components through which UEM Server – client communication travels. They are not security relevant for the purpose of this evaluation since the server-client channels are secured end to end between the TOE components and through the other components. Those other components cannot decrypt or otherwise access information in those secure channels, although they can disrupt or redirect them, like any other components on the Internet.

The UEM Android Client is part of the TOE since Android does not have agents of its own. The UEM Server can manage mobile Android devices through interaction with an enrolled UEM Android Client and can alternately manage mobile iOS devices through interaction with the iOS agent developed and evaluated by Apple.

The Target of Evaluation (TOE) is the BlackBerry Unified Endpoint Management (UEM) Server and Android Client version 12.

The BlackBerry product consists of a UEM Server and UEM Android client (Agent), where the Server provides centralized management of mobile devices and the Agent software (installed on each Android device) enforces the policies of the Server on each device.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

1) The UEM Server (version 12) installed upon the Windows Server 2016 with Java JRE 8.0, using the Microsoft SQL Server 2008-2016.
2) The UEM Android Client version 12 APK installed upon an evaluated Samsung device running Android 9, 8.1, or 8.0. (see Security Target for a mapping to Samsung mobile device evaluations)

3.2 TOE Architecture

The UEM Server consists of a number of services running within the Windows Server 2016 platform. However, only the Core and UI services are included in the TOE for the purpose of evaluation. The other components are either disabled or play no role in any security enforcement.

The UEM Server requires a SQL database to operate and can optionally be configured to utilize an LDAP server for user authentication as well as a SYSLOG server to export audit records. Some other components such as Exchange are not included in the scope of evaluation or are not security relevant – the BBR (Blackberry router) and BlackBerry NOC are network routing components through which UEM Server – client communication travels. They are not security relevant for the purpose of this evaluation since the server-client channels are secured end to end between the TOE components and through the other components. Those other components cannot decrypt or otherwise access information in those secure channels, although they can disrupt or redirect them, like any other components on the Internet.

The UEM Android Client is part of the TOE since Android does not have agents of its own. The UEM Server can manage mobile Android devices through interaction with an enrolled UEM Android Client and can alternately manage mobile iOS devices through interaction with the iOS agent developed and evaluated by Apple. The EMM Agent consists of a single component on evaluated iOS platforms.

3.3 Physical Boundaries

The physical boundaries of the BlackBerry UEM Server and Android Client are the physical perimeter of the servers hosting the UEM Server and the physical perimeter of the mobile devices being managed by the UEM Server (put another way, the mobile devices running the Android Client).

The UEM Server also interacts with Microsoft SQL server and optionally LDAP and SYSLOG servers as described above.

4 Security Policy

This section summaries the security functionality of the TOE:

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

4.1 Security audit

The BlackBerry UEM server is designed to generate and export audit events. The audit events are stored in the SQL database and sent to the configured syslog servers as events occur. The BlackBerry UEM server can also generate alerts for specific events – these alerts are sent to administrators as e-mails. The BlackBerry UEM server supports TLS tunneling of syslog messages to protect exported audit records.

The BlackBerry UEM Android client is also designed to generate and export audit events. It stores audit events in the platform audit logs which it can retrieve and send to its enrolled BlackBerry UEM server. The BlackBerry UEM server will forward the events to a configured syslog server as the events are received. The BlackBerry UEM Android client can also send required alerts directly to the BlackBerry UEM server which are received, logged as audit events, and treated as administrator alerts.

4.2 Cryptographic support

The BlackBerry UEM server uses the Certicom Security Builder GSE-J Crypto Core Module (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3391) for its cryptographic operations. The Certicom Security Builder GSE-J Crypto Core Module provides Cryptographic Algorithm Validation Program (CAVP) certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, encryption/decryption, and cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, initialization vector generation, secure key storage, and key and protected data destruction. The primitive cryptographic functions are used to implement security communication protocols (TLS and HTTPS) used for communication between the Server and Agent and between the Server and remote administrators.

The UEM Android Client uses the cryptographic functions provided by the evaluated mobile devices.

4.3 Identification and authentication

The BlackBerry UEM server requires administrators to login prior to performing any security functions or accessing any services, such as creating an activation password. Similarly, mobile devices must authenticate with the server using an activation password prior to enrolling

Both the BlackBerry UEM server and Android client use X.509 certificates in conjunction with TLS to both authenticate and secure remote connections.

4.4 Security management

The BlackBerry UEM server facilitates granular administrative access to functions based on roles: server primary administrators, security configuration administrators, device user administrators, auditor, and mobile device users. . Administrators access the BlackBerry UEM server via a web-based interface. The BlackBerry UEM server also supports the definition of mobile device users, and upon enrollment each mobile device generates an X.509 certificate used to identify that enrolled device.

The BlackBerry UEM server provides all the features necessary to manage its own security functions as well as to manage mobile device policies sent to enrolled mobile devices (via their clients).

The BlackBerry UEM Android client provides the features necessary to securely communicate and enroll with the BlackBerry UEM server, apply policies received from the BlackBerry UEM server, and report the results of applying policies.

4.5 Protection of the TSF

The BlackBerry UEM server and Android client work together to ensure that all security related communication between those components is protected from disclosure and modification.

The BlackBerry UEM server includes self-testing capabilities to ensure that they are functioning properly as well as to cryptographically verify that their executable images are not corrupted. The UEM server also includes secure update capabilities to ensure the integrity of any updates so that updates will not introduce malicious or other unexpected changes in the TOE.

4.6 TOE access

The BlackBerry UEM server has the capability to display an advisory banner when users attempt to login in order to manage the TOE.

4.7 Trusted path/channels

The BlackBerry UEM server uses TLS/HTTPS to secure communication channels between itself and remote administrators and mobile device users accessing the server via a web-based user interface. It also uses TLS to secure communication channels between itself, enrolled devices, its configured SQL database server, syslog servers, and optionally configured LDAP servers.

The following is a summary of applicable secure channels:

1. UEM server console used by administrators – TLS not subject to mutual X.509 authentication. Certicom implementation of TLS on server.
2. Mobile device UEM client to UEM server – TLS not subject to mutual X.509 authentication for initial enrollment, but always uses mutual X.509 authentication once enrolled. Certicom implementation of TLS on server – Mobile device implementation of TLS on the client end.
3. UEM server to SQL database, SYSLOG and LDAP – TLS optionally configured for mutual X.509 authentication. Certicom implementation of TLS on server. Communication with the SQL database is either local within the Windows platform on which the UEM server executes, or protected by IPsec provided by the Windows platform.

5 Assumptions

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

- Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 (MDMPP40)
- PP-Module for MDM Agents, Version 1.0, 2019-04-25 (MDMA10)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)

That information has not been reproduced here and the MDMPP40/MDMA10/ PKGTLS11 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 MDMPP40/MDMA10/ PKGTLS11 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:

- 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.

7 Documentation

The following documents were available with the TOE for evaluation:

- BlackBerry UEM Administrative Guidance Document, UEM Version 12.12, March 2020

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 (MDMPP40/MDMA10/ PKGTLS11) for BlackBerry UEM Server and Android Client Version, Version 0.3, 28 April 2020 (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 MDMPP40/MDMA10/ PKGTLS11 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration consists of a collection of server components (MDM server) and mobile device applications (MDM agent).

To use the product in the evaluated configuration, the product must be configured as specified in the following documents.

- BlackBerry UEM Administrative Guidance Document, UEM Version 12.12, March 2020

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.

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 5 and CEM version 3.1 rev 5. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

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 BlackBerry UEM Server and Android Client Version 12 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 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 MDMPP40/MDMA10/ PKGTLS11 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 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 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 ran the set of tests specified by the assurance activities in the MDMPP40/MDMA10/ PKGTLS11 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 performed a public search for vulnerabilities on 04/17/2020 and did not discover any public issues with the TOE. The terms used for the search were as follows:

- BlackBerry
- Certicom Security Builder
- GSE-J
- UEM
- JRE
- LDAP
- TLS

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 validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the BlackBerry UEM Administrative Guidance Document. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness for this evaluation.

12 Annexes

Not applicable

13 Security Target

BlackBerry UEM Server and Android Client Version (MDMPP40/MDMA10/PKGTLS11) Security Target, Version 0.6, 28 April 2020.

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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 (MDMPP40), PP-Module for MDM Agents, Version 1.0, 2019-04-25 (MDMA10), and Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)

[5] BlackBerry UEM Server and Android Client Version (MDMPP40/MDMA10/PKGTLS11) Security Target, Version 0.6, 28 April 2020 (ST)

[6] Assurance Activity Report (MDMPP40/MDMA10/PKGTLS11) for BlackBerry UEM Server and Android Client Version 12, Version 0.3, 28 Aprilf 2020 (AAR)

[7] Detailed Test Report (MDMPP40/MDMA10/ PKGTLS11) for BlackBerry UEM Server and Android Client Version, Version 0.3, 28 April 2020 (DTR)

[8] Evaluation Technical Report for BlackBerry UEM Server and Android Client Version 12, ETR Version 0.3, 28 April 2020 (ETR)

[9] BlackBerry UEM Administrative Guidance Document, UEM Version 12.12, March 2020