National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
BlackBerry UEM Server and Android Client v12

Report Number: CCEVS-VR-VID11427-2024
Dated: May 30, 2024
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
Randy Heimann
Clare Parran
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Douglas Kalmus
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of BlackBerry UEM Server and Android Client v12 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 Columbia, MD, United States of America, and was completed in May 2024. 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 PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 27 January 2020 which includes the Base PP: Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMA10) with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019 (PKGTLS11).

The Target of Evaluation (TOE) is the BlackBerry UEM Server and Android Client v12.

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 technical information included in this report was obtained from the BlackBerry UEM Server and Android Client v12 Security Target, version 0.93, May 29, 2024 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	BlackBerry UEM Server and Android Client v12
Protection Profile	PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 27 January 2020 (CFG_MDM-MDM_AGENT_V1.0) which includes the Base PP: Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40) and the PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMA10) with the Functional Package for Transport Layer Security, Version 1.1, 1 March 2019 (PKGTLS11)
ST	BlackBerry UEM Server and Android Client v12 Security Target, version 0.93, May 29, 2024
Evaluation Technical Report	Evaluation Technical Report for BlackBerry UEM Server and Android Client v12, version 0.3, May 29, 2024
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.
Developer	BlackBerry Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Sheldon Durrant, Randy Heimann, Clare Parran, Lori Sarem

Table 1: Evaluation Identifiers

3 Assumptions & Clarification of Scope

Assumptions

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

- Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019 (MDMPP40)
- PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMA10)
- Functional Package for Transport Layer Security, 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.

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 Management Protection Profile with the MDM Agents PP-Module and the TLS Functional 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.
- Apart from the Admin Guide, additional customer documentation for the specific Mobile Device Management and Agent models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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 MDMPP40/MDMA10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

4 Architectural Information

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

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

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.

4.1 TOE Description

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 or Windows Server 2019 with Java JRE 8.0. Ideally, the scope of supported platforms for the evaluation would be Windows Server 2016 or Windows Server 2019 wherever they are deployable, however, it will be limited due to NIAP policy about CAVP algorithm certificates – the allowed environments would be expected to conform to the environments of the CAVP certificates (e.g., using the processors used for CAVP algorithm testing). In this case, the CAVP testing for Certicom was done on Windows Server 2016 and Windows Server 2019 running in a virtual environment (VMWare ESXi 7) on an Intel Xeon E5-2620**.**

The BlackBerry UEM Android Client has two main deployment methods– as a single Workspace client or alternate as a dual client with one managing the Personal (whole) device and another managing the Workspace. There is one BlackBerry UEM client deployment per enrolled mobile device. The scope of supported managed client devices for the evaluation is limited by the set of devices evaluated on the NIAP PCL[1]:

- Android 13 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11342,
- Android 12 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11307 and,
- Android 12 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11228.

Since the iOS agents are evaluated as part of the Apple iOS evaluations, the UEM server will be tested to ensure it can manage those devices, but the agent’s behavior on those devices will not otherwise be tested. The support is limited by the set of devices evaluated on the NIAP PCL:

- iOS 15 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11237, and
- iOS 16 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11349.

4.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 7 below.

[1] Note that the oldest evaluation listed here was removed from the NIAP PCL late in the evaluation of this product, but the applicable devices remain supported and tested in the context of this evaluation.

4.3 TOE Architecture

As depicted above 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 BlackBerry NOC is a network routing component 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.

4.4 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.

5 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

5.1 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.

5.2 Cryptographic support

The BlackBerry UEM server uses the Certicom Security Builder FIPS Java Module for its cryptographic operations. It includes the following algorithm certificates which are applicable as the platform for this evaluation:

AES	A5201
DRBG	A5201
ECDSA	A5201
HMAC	A5201
KAS	A5201
RSA	A5201
SHS	A5201

The BlackBerry UEM Android client uses the cryptographic functions provided by the evaluated mobile devices. As such, the Android client can reference the applicable certificates in the preceding evaluations of those devices.

The BlackBerry UEM server implements a X.509 key hierarchy summarized as follows:

1. The PKI is rooted in a self-signed certificate (RSA 4096 SHA512) created when the first server is installed.

2. The root is used to issue an intermediate CA certificate (RSA 3072 SHA512) also created when the first server is installed.
3. Additional certificates are issued using the intermediate CA certificate as follows:
    a. Console web server certificate (RSA 2048 SHA512)
    b. Server client certificate (RSA 2048 SHA512) – used for SYSLOG, LDAP, etc.
    c. Profile signing certificate (RSA 2048 SHA512) – used for Apple MDM
    d. Per-device BDMI payload signing key (RSA 3072 SHA512)
    e. Per-device enrolled device certificates - issued during enrollment (RSA 2048 SHA512)
4. All of the certificates above, except the per-device certificates, are stored in the SQL database and the key store is encrypted with a DEK (AES-CBC 256) also created during installation. The per-device BDMI keys are encrypted using the DEK separately from the rest of the key store. The DEK is encrypted using an EC secp512r1 key (stored in the Windows key store), that is unique to each unit of scale (created during installation), and stored on the local file system of each unit of scale.
5. Each individual certificate in the key store is also encrypted individually using a DEK created during installation using PBEWithHmacSHA256AndAES256 (AES-CBC mode).
6. The enrolled device certificate private keys are generated on the mobile device and signed by the intermediate CA on the applicable UEM server.
7. Additional trusted root CAs can be loaded to support accepting certificates from other devices (syslog, ldap, etc.).

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

6 Documentation

The following documents were available with the TOE for evaluation:

- BlackBerry UEM Administrative Guidance Document, Version 12.19, May 2024

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 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 document:

- BlackBerry UEM Administrative Guidance Document, Version 12.19, May 2024

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 for BlackBerry UEM Server and Android Client v12, Version 0.3, May 29, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 a Common Criteria Certification document and ran the tests specified in the MDMPP40/MDMA10/PKGTLS11 including the tests associated with optional requirements.

9 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 5 and CEM version 3.1 rev 5. The evaluation determined the UEM Server and Android Client v12 TOE to be Part 2 extended, and to meet the SARs contained in the MDMPP40/MDMA10/PKGTLS11.

9.1 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 v12 products that are consistent with the Common Criteria, and product security function descriptions that support 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.

9.2 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 MDMPP40/MDMA10/PKGTLS11 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.

9.3 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 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.

9.4 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 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.

9.5 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 MDMPP40/MDMA10/PKGTLS11 and recorded the results in a Test Report, 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.

9.6 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: “BlackBerry”, “Certicom Security Builder”, “GSE-J”, “Unified Endpoint Management”, “Java runtime environment”, “LDAP”, and “TLS”.

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.

9.7 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.

10 **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, Version 12.19, May 2024* document and any additional guidance that it references. 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 ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 **Security Target**

The Security Target is identified as: *BlackBerry UEM Server and Android Client v12 Security Target, Version 0.93, May 29, 2024*.

13 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 2: Glossary

14 **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, 25 April 2019 (MDMPP40).

[5] PP-Module for Mobile Device Management Agents, Version 1.0, 25 April 2019 (MDMA10).

[6] Functional Package for Transport Layer Security, Version 1.1, 1 March 2019 (PKGTLS11).

[7] BlackBerry UEM Server and Android Client v12 Security Target, Version 0.93, May 29, 2024 (ST).

[8] BlackBerry UEM Administrative Guidance Document, Version 12.19, May 2024 (AGD).

[9] Assurance Activity Report for BlackBerry UEM Server and Android Client v12, Version 0.3, May 29, 2024 (AAR).

[10] Detailed Test Report for BlackBerry UEM Server and Android Client v12, Version 0.3, May 29, 2024 (DTR).

[11] Evaluation Technical Report for BlackBerry UEM Server and Android Client v12, Version 0.3, May 29, 2024 (ETR).