Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1235-2025

for

BlackBerry Unified Endpoint Management (UEM) Server Version 12.21.1 (40.32.0)

from

BlackBerry Ltd.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1235-2025 (*)

Mobile Device Management Server

BlackBerry Unified Endpoint Management (UEM) Server

Version 12.21.1 (40.32.0)

from	BlackBerry Ltd.
PP Conformance:	Protection Profile Mobile Device Management - Trusted Server (MDM-TS). Version 1.0 as of 2021-09-27; BSI-CC-PP-0115-2021, PP-Configuration Mobile Device Management - Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC). Version 1.0 as of 2021-09-27; BSI-CC-PP-0116-2021
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
valid until:	7 September 2030

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 8 September 2025

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Fabian Hoduschek
Head of Certification

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz – BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs – Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) – dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

[4] Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product BlackBerry Unified Endpoint Management (UEM) Server, Version 12.21.1 (40.32.0) has undergone the certification procedure at BSI.

The evaluation of the product BlackBerry Unified Endpoint Management (UEM) Server, Version 12.21.1 (40.32.0) was conducted by atsec information security GmbH. The evaluation was completed on 28 August 2025. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: BlackBerry Ltd.

The product was developed by: BlackBerry Ltd.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation [10] and in the following report, are observed,
- the product is operated in the environment as specified in the following report and in the Security Target [5].

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target [5]. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis. Therefore, the BSI reserves the right to revoke the certificate, especially if an exploitable vulnerability of the certified product gets known.

In order to avoid an indefinite usage of the certificate when evolved, attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 September 2025 is valid until 7 September 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target [5] and user guidance documentation [10] mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product BlackBerry Unified Endpoint Management (UEM) Server, Version 12.21.1 (40.32.0) has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] BlackBerry Ltd.
2200 University Avenue East
Waterloo, Ontario, N2K 0A7
Canada

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is BlackBerry Unified Endpoint Management (UEM) Server Version 12.21.1 (40.32.0), a software for centralized management of mobile devices such as smartphones and tablets that are used in an organization.

The Security Target [5] is the basis for this certification. It is based on the certified Protection Profile Mobile Device Management - Trusted Server (MDM-TS) [7] and the PP-Configuration complemented with the PP-Module Trusted Communication Channel (TCC) [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus, the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF.AUDIT - Security Audit	The TOE implements automated logging based on the actions as specified in the Security Target [5], including device enrolment/unenrolment and MDM server start-up and shutdown.
SF.CRYPTO – Cryptographic Support	The TOE uses the Certicom Security Builder GSE-J Crypto Core (version 2.9.2) for its generation and verification of RSA and ECDSA signatures, to perform SHA-based HMAC, AES encryption and decryption, SHA hashing as well as to establish TLS/HTTPS connections, generate Ivs, and generate random data. To seed its DRBG the Jitter RNG version 3.0.0 is utilized.
SF.DP - User Data Protection	The TOE implements an internal PKI to support the issuance of certificates for its own use (i.e., to identify itself to other parties) and to be sent to mobile devices during enrolment. Mobile devices may be grouped and assigned to different managers by utilizing different parameters of a device, i.e. in the TOE scope are Operating System (OS), Operating System Version (OSV), Device Model (DM) and Manufacturer (M). Payloads (i.e. new or updated policies and commands) are sent to the mobile devices over-the-air using a TLS channel during the mobile clients next check-in to the TOE. Managers can also initiate an immediate check-in using the TOE's Management console. Each device policy is signed by the UEM server using an RSA certificate issued for that purpose.
SF.IA - Identification and authentication	For each administrative account, the TOE stores the role including the permissions and the mobile device users and user groups managed by the user. For mobile devices enrolled in the TOE, the mobile device user who activated the device and the device group to which the mobile device has been assigned to are stored. The TOE supports the creation of local users, but also allows to use users maintained by an LDAP server. Furthermore, staff members cannot perform any actions at all (other than logging in, requesting password recover, choosing a

TOE Security Functionality	Addressed issue
	language and selecting the authentication provider) until they authenticated successfully.
SF.MGMT - Security management	The TOE maintains a set of pre-configured roles and allows to create custom roles. Each role has its unique set of permissions and actions it is allowed to take.
SF.PT - Protection of the TSF	Data transmitted between the Management console (TLS client) and the Core Server component (TLS server) is protected against unauthorized disclosure and modification through the use of TLS with mutual, certificate-based authentication. Furthermore, the data channel between the staff agents and the device agents is also protected against unauthorized disclosure and modification using TLS.
SF.CHANNEL - Trusted path/channels	The TOE implements TLS v1.2 to secure communication channels with device agents during enrolment, with all enrolled device agents, remote staff agents, remote database server as well as external audit and LDAP authentication servers. For all TLS channels, the TOE supports mutual authentication using X509v3 certificates, however, mutual authentication is always required for enrolled device agents, as well as external audit and LDAP servers.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5] and [8], chapter 3. Based on these assets the TOE Security Problem is defined in terms of Threats, Organisational Security Policies and Assumptions. This is outlined in the Security Target [5], chapters 3.1, 3.2 and 3.3 respectively.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

BlackBerry Unified Endpoint Management (UEM) Server, Version 12.21.1 (40.32.0)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Installation package for installation of the TOE: BlackBerry Unified Endpoint Management (UEM) Server Filename: UEM-12.21.1.zip sha-256 hash: 76e9331fe24b04e0b6472dbd7df15bdffcfe28ebf80a2ba7cc0c1c099f77ba60	12.21.1 (40.32.0)	Download
2	DOC	BlackBerry UEM Administrative Guidance Document [10] filename: BlackBerry_UEM_AGD v1.14.pdf	Version 1.14 Date 2025-08-18	Download
3	DOC	Mobile device policies sheet [11] filename: Policy-Reference-Spreadsheet-BlackBerry-UEM.xlsx	Version 12.20	Download

Table 2: Deliverables of the TOE

The delivery of the TOE is electronic download in the form of an installation package. The download is only possible after the customer logs in to the myAccount Portal, which provides TLS-protected communication. The developer operates the download site (myAccount Portal) and provides a SHA-256 hash for the installation package to be downloaded that enables the customer to verify the integrity of the download.

The documentation can be downloaded via a web page operated by the developer and is also protected via TLS.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements a role-based access control policy to control administrative access to the system.

In addition, the TOE implements a security policy for device attendants grouping and cluster of groupings for the manager attendant allowing the grouping of device attendants and managing of the cluster.

Specific details concerning the above-mentioned security policies can be found in the Security Target [5], chapter 6.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.PROPERSTAFF, OE.PROPERUSER, OE.PROPERMANAGEMENT, OE.RESILIENCE, OE.DEVICELIFECYCLE, OE.SUPPORTINGSERVICES, OE.RELIABLETIMESTAMPS and OE.AUDITTRAIL

Details can be found in the Security Target [5], chapter 4.2.

5. Architectural Information

The Target of Evaluation is the software application BlackBerry UEM Server, developed by BlackBerry Limited. The TOE is software-only and is accompanied by administrative guidance documentation [10].

The hardware, the virtualization, the platform OS, the Java Runtime Environment and the SQL database as well as additional software needed for TOE operation are considered to be part of the TOE environment.

The TOE is accessible via network connection, administration is conducted via the Web UI interface or automated via the Web Service API.

The TOE consists of two subsystems, namely the UEM Core and the Management console. Both subsystems are constituted of multiple modules.

The UEM Core subsystem is designated as the central subsystem of the TOE implementing the majority of the security functionality:

- Logging, monitoring, reporting, eventing and management functions,
- authentication, authorization, encryption services, scheduling, sending commands, IT policies and profiles to devices,
- sending user, policy and other configuration data,
- communication with the Management Console subsystem, access to external services like the SQL database.

The Management Console provides a web-based administrator interface to manage system settings, users, and devices.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

Testing was conducted on Systems and in an environment conforming to the evaluated configuration as outlined in Chapter 8.

Developer Testing

The developer performed testing against all interfaces of the TOE, including optional interfaces, i.e. LDAP and SYSLOG testing. All tests are manual tests triggered or verified via user-visible interfaces; this also includes manual checks of logs and database settings.

Overall, the developer executed 153 tests, including test variations based on the different supported platforms, i.e. iOS and Samsung Knox.

The developer used a mapping between TSFI and test cases with related SFRs and classification as well as a mapping between subsystems and test cases with related SFRs to ensure that all security-relevant interfaces, subsystems and all SFRs have been subject to testing.

All developer test cases were executed successfully and showed the expected results.

Evaluator Testing

The evaluator rerun part of the developer tests and devised several additional independent tests regarding audit data filtering, device groups, device group permission, unsupported TLS cipher suites (client), unsupported TLS versions (client), certificate validation, OCSP state, OCSP certificate revocation and access of defined roles.

The tests were mainly defined to exercise TSFI specifications as well as SFR functionality and claimed in the TOE documentation.

All tests were successfully executed without relevant deviations.

Penetration Testing

The evaluator devised tests, which intent to analyse a proper error handling of the TOE by implementing tests using the interfaces of the TOE. Specifically, the evaluator tested the TLS protocol as well as the access control mechanisms of the TOE. In contrast to the automated functional testing these tests were mostly manual test cases.

All tests results were accepted by the evaluator. Thus, the evaluator concluded that the TOE with respect to the tested functionality behaves as defined in the Security Target [5].

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration is covered in section 1.2.2 of the BlackBerry UEM Administrative Guidance Document [10] and in section 1.5.2 of the Security Target [5]. These documents detail hardware, OS, virtualization, Java version, and database essential for the installation as well as additional components needed for operation.

For testing the following components were used: A test system with an AMD EPYC 7702P processor, VMware ESXi 8.0.2, Windows Server 2022, Microsoft SQL Server 2017, OpenJDK 17 including the Java JRE 17 and Microsoft 2019 Active Directory.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile Mobile Device Management - Trusted Server (MDM-TS). Version 1.0 as of 2021-09-27; BSI-CC-PP-0115-2021 [7]

PP-Configuration Mobile Device Management - Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC). Version 1.0 as of 2021-09-27; BSI-CC-PP-0116-2021 [8]

- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table in annex B of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEM	Unified Endpoint Management

13.2. Glossary

Augmentation – The addition of one or more requirement(s) to a package.

Collaborative Protection Profile – A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension – The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal – Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal – Expressed in natural language.

Object – A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package – named set of either security functional or security assurance requirements

Protection Profile – A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target – An implementation-dependent statement of security needs for a specific identified TOE.

Subject – An active entity in the TOE that performs operations on objects.

Syslog – A standard for message logging within computer networks.

Target of Evaluation – An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality – Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation/CC
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology

ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] Security Target BSI-DSZ-CC-1235-2025, Version 1.9, 2025-08-18, Security Target for BlackBerry UEM Server, BlackBerry Ltd.

[6] Evaluation Technical Report, Version 1, 2025-08-19, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[7] Protection Profile Mobile Device Management - Trusted Server (MDM-TS). Version 1.0, 2021-09-27; BSI-CC-PP-0115-2021

[8] PP-Configuration Mobile Device Management - Trusted Server (MDM-TS) complemented with PP-Module Trusted Communication Channel (TCC). Version 1.0, 2021-09-27; BSI-CC-PP-0116-2021

[9] Configuration list for the TOE, Archive “alc/ALC_CI_List_2025-06-16.zip”, dated 2025-06-16, BSI Evaluation CI list (confidential document)

[10] Guidance documentation for the TOE, Version 1.14, 2025-08-18, BlackBerry UEM Administrative Guidance Document, BlackBerry Ltd.

[11] Mobile device policies sheet, file Policy-Reference-Spreadsheet-BlackBerry-UEM.xlsx, Version 12.20, as delivered on 2025-08-19, BlackBerry Ltd.

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria in its CCRA Documents can be followed:

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1235-2025

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Authentication (Server)	X.509 certificates	[RFC5280]	N/A	-	
2		RSA signature verification RSASSA-PKCS1-v1.5 using SHA-2	[RFC3447] (PKCS#1 v2.1) [FIPS186-4][9] (RSA) [FIPS180-4] (SHA)	Modulus length: >= 2048 bits	No[8]	Security Level above 100 bits
3		RSA signature verification RSASSA-PSS using SHA-2	[RFC3447] (PKCS#1 v2.1) [FIPS186-4][9] (RSA) [FIPS180-4] (SHA)	Modulus length: >= 3072 bits	Yes	
4	Authentication (Client)	RSA signature verification RSASSA-PKCS1-v1.5 using SHA-2	[RFC3447] (PKCS#1 v2.1) [FIPS186-4][9] (RSA) [FIPS180-4] (SHA)	Modulus length: >= 3072 bits	Yes	
5		RSA signature verification RSASSA-PSS using SHA-2	[RFC3447] (PKCS#1 v2.1) [FIPS186-4][9] (RSA) [FIPS180-4] (SHA)	Modulus length: >= 3072 bits	Yes	
6		ECDSA signature verification using SHA-2 with the same size as the selected curve	[FIPS186-4][9] (ECDSA) [FIPS180-4] (SHA)	Key size defined by selected curve size: 256, 384 or 521 bits	Yes	
7	ECC key generation for use in ECDH	ECDSA NIST P-256, P-384, P-521	[FIPS186-4] B.4	Key size defined by selected curve size: 256, 384 or 521 bits	Yes	

[8] The TOE accepts RSA certificates with a modulus length below 3072 bits for external services, like push notification, as some of this services cannot be used without this. It enforces the use of 3072 bits and higher for keys it is controlling. This includes keys generated by it and configured for bi-directional authentication between TOE components as well as with the remote devices. For these keys a Security Level above 120 Bits is achieved.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
8	RSA key generation	RSA key generation	[FIPS186-4][9] B.4	Modulus length: >= 3072 bits	Yes	
9	Key establishment: Key agreement Ephemeral	TLS_ECDHE with NIST P-256, P-384, P-521	[SP800-56A-rev3] [RFC5289]	Key size defined by selected curve size: 256, 384 or 521 bits	Yes	
10	Key derivation	TLS v1.2 PRF: HMAC with SHA-256, SHA-384	[RFC2104] (HMAC) [FIPS180-4] (SHA) [RFC5246] (TLSv1.2)	variable	-	
11	Confidentiality of user data	Cipher: AES Modes: GCM	[FIPS197] (AES) [SP800-38D] (GCM) [RFC5289] (AES GCM within TLS) [RFC5246] (TLSv1.2)	|k| = 128, 256	Yes	
12	Confidentiality of user data	Cipher: AES Modes: CBC	[FIPS197] (AES) [SP800-38A] (CBC)	|k| = 256	Yes	
13	Trusted Channel	TLS v1.2	[RFC5246]		-	
14	Random number generation	Hash DRBG with SHA-512 core, no PR	[SP800-90A-Rev1]		-	

Table 3: TOE cryptographic functionality

References for table 3

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/pubs/fips/180-4/upd1/final

FIPS186-4[9] **Digital Signature Standard (DSS)**
Date 2013-06-19
Location https://csrc.nist.gov/pubs/fips/186-5/final

FIPS197 **Advanced Encryption Standard (AES)**
Date 2023-05-09
Location https://csrc.nist.gov/pubs/fips/197/final

[9] Note that FIPS 186-5 requirements are fullfilled: Albeit the PP and as a result the ST contains the claim to implement FIPS 186-4, the CAVP testing of the asymmetric algorithms covered FIPS 186-5 as well. Therefore, the FIPS186-5 requirements are fullfilled as well.

RFC2104 **HMAC: Keyed-Hashing for Message Authentication**
Author(s) H. Krawczyk, M. Bellare, R. Canetti
Date 1997-02-01
Location http://www.ietf.org/rfc/rfc2104.txt

RFC3447 **Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**
Author(s) J. Jonsson, B. Kaliski
Date 2003-02-01
Location http://www.ietf.org/rfc/rfc3447.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**
Author(s) T. Dierks, E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5246.txt

RFC5280 **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
Author(s) D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk
Date 2008-05-01
Location http://www.ietf.org/rfc/rfc5280.txt

RFC5288 **AES Galois Counter Mode (GCM) Cipher Suites for TLS**
Author(s) J. Salowey, A. Choudhury, D. McGrew
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5288.txt

RFC5289 **TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)**
Author(s) E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5289.txt

RFC7919 **Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)**
Author(s) D. Gillmor
Date 2016-08-01
Location http://www.ietf.org/rfc/rfc7919.txt

SEC2 **Recommended Elliptic Curve Domain Parameters**
Date 2000
Location http://www.secg.org

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Technique**
Date 2001-12-01
Location https://csrc.nist.gov/pubs/sp/800/38/a/final

SP800-38D **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
Date 2007-11-28
Location https://csrc.nist.gov/pubs/sp/800/38/d/final

SP800-56A-Rev3 **Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography**
Date 2018-04-16
Location https://csrc.nist.gov/pubs/sp/800/56/a/r3/final

SP800-90A-Rev1 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
Date 2015-06-24
Location https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

Note: End of report