BlackBerry Enterprise Solution for Microsoft Exchange Security Analysis

Fraunhofer SIT

Certification Report
06-104302

Fraunhofer Institut
Sichere Informations-
Technologie

Table of Contents

Executive Summary

Research In Motion (RIM) engaged Fraunhofer Institute for Secure Information Technology (SIT) to conduct an in-depth security evaluation of the BlackBerry® Enterprise Solution in the institute's IT Security Testlab. The evaluators used confidential design documents provided by RIM and performed an extensive hands-on analysis of the solution's components, interfaces, software platform, environment and protocols. The Fraunhofer Institute SIT IT Security Testlab inspected all aspects of encryption, key exchange, smartphone management and server security, used SIT testing tools and made suggestions for further improving BlackBerry security. RIM has already included these suggestions in the product.

The overall aim of the passed security analysis was to evaluate the BlackBerry Enterprise Solution against well-accepted principles of the IT security community. Fraunhofer Institute SIT testifies the solution's compliance with state-of-the-art security, provided the published configuration of the solution is used according to Fraunhofer recommendations. Among these recommendations is that companies should change the standard BlackBerry smartphone encryption setting to use AES encryption, and modify the server setup. Adhering to Fraunhofer configuration provides strong protection against known attack methods. It results in a loss of some management features, but does not reduce core functionality.

The evaluation also identified possible ways for RIM to further minimize the potential impact of successful attacks. No actual vulnerabilities are known to the evaluators. However, residual risks for consideration in the corporate risk management process are identified.

1 Introduction

The security of IT systems is a mission critical factor in the enterprise context. The quintessential requirements for reaching a higher degree of IT security are: considerable consciousness of IT risks, a holistic point of view and a security assessment of the assigned IT systems by developer-independent testers. On the basis of its longstanding experience evaluating IT security, Fraunhofer Institute for Secure Information Technology (SIT) developed a methodology for IT security assessments in different evaluation depths which considers the entire solution and is used in projects of the IT Security Testlab of Fraunhofer Institute SIT.

Research In Motion (RIM) engaged Fraunhofer Institute SIT to perform an in-depth security evaluation of the BlackBerry Enterprise Solution including deep analysis of the solution's components, interfaces, processes, software platform, environment and protocols. RIM provided Fraunhofer Institute SIT with access to highly confidential information to allow Fraunhofer Institute SIT to rigorously review the solution.

The security analysis was carried out as three major projects. The first project analyzed the security of the communication between the major components of the BlackBerry Enterprise Solution: the BlackBerry® Enterprise Server, BlackBerry smartphone and BlackBerry® Infrastructure. The second project analyzed the security of the interaction between the individual components of the BlackBerry Enterprise Server and the processes involved. The third project focused on the BlackBerry smartphone and the analysis of relevant physical and logical interfaces to the smartphone and its environment, such as the Internet. In addition to the communication content and processes, the project team also evaluated the security of standard applications of the BlackBerry Enterprise Solution, such as email attachment viewing, access and integration of corporate data sources and the use of PIM applications.

The security analysis assumed extensive security demands were present for corporate users. Fraunhofer Institute SIT defined the protection goals, developed the attacking scenarios and performed attacks and manipulation attempts in practice. The tests were conducted in a typical reference installation in the institute’s IT Security Testlab with expert IT security knowledge and intimate knowledge of the BlackBerry Enterprise Solution based on the design documents provided by RIM.

2 Security Analysis

The basic evaluation principle applied in this security analysis is that a secure IT system should not exhibit relevant security flaws in its typical application context. The protection should be equally high with respect to all components, processes and interfaces and should be based — from a generalized perspective — on secret tokens rather than secret algorithms. This principle should require the cryptographic protection to unfold its strength to secure the solution as a whole, making the security measurable by the strength of well-engineered and approved cryptographic algorithms.

Within the evaluation process of the BlackBerry Enterprise Solution components, processes and interfaces were systematically studied with knowledge of common software vulnerabilities, state-of-the-art attack techniques and SIT analysis tools, as well as design documents provided by RIM. The security of the solution was not only evaluated by checking different isolated security mechanisms, the evaluation considered combinations of potential flaws that could facilitate a major attack, as well as potential vulnerabilities in distinct parts. Unlike standard tests, the security evaluation focused on the uncovering of such hidden dangers.

Since the utilization and deployment of technology within an organization can impact overall network security, the BlackBerry Enterprise Solution Security Evaluation examined security in a typical BlackBerry deployment environment. The depth of the examination of the components depended on the expected impact as well as on the threats outlined.

2.1 Evaluation Object and Environment

The evaluated BlackBerry Enterprise Solution is a mobile messaging solution providing email push capability, attachment viewing, organizer functions, special browsing abilities and instant messaging. In the tested scenario, the solution is integrated within existing corporate email accounts as a wireless extension of the current email service.

The evaluation object consists of all components of the BlackBerry Enterprise Solution architecture fulfilling the usage scenarios mentioned above. The primary components of this architecture are the BlackBerry smartphone, the BlackBerry Infrastructure and the BlackBerry Enterprise Server.

The different components were evaluated separately to address their individual interfaces and specific tasks within the BlackBerry Enterprise Solution. The evaluation, however, focused on providing results about the security of the overall system and its secure interaction with its environment.

The environment used during the evaluation consisted of a corporate intranet with a messaging server, in particular the Microsoft® Exchange Server, and access to the Internet. The intranet was protected by the corporate firewall.

Component Deployment and Network Environment

The test environment consisted of a separated network within the institute's IT Security Testlab. The installation was comprised of three PCs, each of them installed with Microsoft Windows Server® 2003 SE SP1 or Windows® XP SP2, and with Microsoft Terminal Services enabled using the Remote Administration mode. The first server hosted the Microsoft Exchange Server software and domain services, whereas the second machine ran the BlackBerry Enterprise Server in its default component distribution configuration. Thus, all BlackBerry Enterprise Server services were configured to be installed and executed on one machine in coordination with the Microsoft® SQL Server® Desktop Engine (MSDE). The third host was used as a client workstation, and ran the BlackBerry® Desktop Manager software and Microsoft® Outlook® 2003.

All the machines in the test environment were attached to a network switch that was assigned to a special VLAN limiting network access. The firewall rules for this VLAN were set up to allow Internet access, including the initialization of a two-way TCP/IP connection to an external server on port 3101 for the BlackBerry Enterprise Server.

Wireless Network Environment

The wireless network environment used in this evaluation fulfilled the following characteristics: The tested BlackBerry smartphones were attached to the T-Mobile Germany GPRS / EDGE network, each smartphone was assigned a public IPv4 address, and was reachable from the Internet concerning UDP and TCP traffic, and firewalls at the wireless network provider did not perform any traffic filtering.

This setup was chosen to provide increased possibilities for network tests. It does not equal the regular network environment used by standard BlackBerry SIMs provided by T-Mobile. Regular T-Mobile BlackBerry smartphones differ from the network test environment configuration in that they are using an APN that does not assign public IP addresses to the BlackBerry smartphones.

Note that using a non-public IP address is a mandatory premise to be inline with the certified configuration.

The wireless network configuration given in the analysis may differ in details from other mobile network providers offering production BlackBerry services.

Environment Installation and Configuration

The BlackBerry Enterprise Server was established using its default installation and update procedures. The server was configured to use the certified configuration parameters presented in section 3.2. Beside this, no settings were changed from the default server configuration. There was no security relevant extra configuration done during the setup or usage to raise the security level of the BlackBerry Enterprise Solution to achieve any advantage for this security analysis.

All BlackBerry smartphones were registered at the BlackBerry Infrastructure named BlackBerry Security Test Infrastructure. The wireless access through the Internet to this non-production BlackBerry Infrastructure was provided by a T-Mobile APN.

The BlackBerry Manager allows the specification of several policy templates to be assigned for different groups of smartphone users. For the analysis, the default policy template was chosen and modified to comply with the certified configuration documented in section 3.2.

2.2 Evaluation Process

In general, the BlackBerry Enterprise Solution Security Analysis was comprised of the definition of the security requirements and a comprehensive threat analysis. Similar to formal certification, test criteria were specified in a Target of Evaluation (TOE)-dependent manner. In each of the three consecutive projects, the threat analysis determined, from a generic perspective, which conditions and risks could arise, and which part of the inspected TOE could be exposed to dangers. The methodology for the identification of threats, protection goals and security characteristics is comparable but not identical to the accepted Common Criteria (CC) proceeding. By means of these initial considerations, a process orientated analysis was conducted. The causal connections between alleged weak points and possible damage potentials were examined therein by prospective analysis.

The evaluation process pattern of each of the three projects was divided into four phases. Phase one of each project provided an overview of the architecture and the components involved, their corresponding interfaces, applied security mechanisms, and the procedures in place.

Phase two described potential threats to the TOE in coordination with protection goals that form the basis for the definition of security requirements. General and specific risks were determined from the security requirements, resulting in the specification of attack scenarios.

Phase three analyzed the potential security impacts on the evaluation object and its environment by executing the attack scenarios, periodically cycled to include new observations discovered during attacks. To execute the scenarios, automatic and manual tools were used to find potential weaknesses.

Finally, phase four concluded the results by summarizing the gathered facts. Additionally, suggestions were provided to further increase the security for identified risks and to fulfill the certification requirements.

Throughout the BlackBerry Enterprise Solution analysis, the overall security was considered the main priority. It was carried out in coordination with the targets of each of the three projects aiming to provide assurance about the observed BlackBerry Enterprise Solution security. Based on this approach, the distinct projects were designed to build the foundation that enables the evaluators to provide statements about the observed overall security.

2.3 Evaluation Depth

The BlackBerry security evaluation was based on available and undisclosed documentation about the BlackBerry system components, interfaces and procedures, as well as design documents provided by RIM. The evaluation was conducted with a black box security test in Fraunhofer Institute SIT's IT Security Testlab, focusing on the whole solution and its implementation.

Proceedings and test criteria were based on recognized procedures, existing protection profiles and validated research results. Information and principles from evaluation methodologies, for example, the Common Criteria for Information Technology Security, were considered, where appropriate.

In comparison to the Evaluation Assurance Level (EAL) of Common Criteria for Information Technology Security Evaluation it has to be differentiated between the various aspects of the analysis at Fraunhofer Institute SIT's IT Security Testlab. The depth of the BlackBerry Enterprise Solution Security Analysis concerning the implementation is comparable with EAL3 to EAL4. Fraunhofer Institute SIT conducted extensive hands-on tests with knowledge of the underlying design documentation. For example, the communication stack was inspected in-depth on all layers, employing Fraunhofer Institute SIT-developed tools, for an efficient and comprehensive evaluation. Besides comparisons of the observed communication with the supplied design specifications of the stacked protocols, the communicated data was manipulated and hand-crafted to test its robustness against malformed packets as well as to check for impacts on security logic caused by Fraunhofer Institute SIT attacks. This interaction with communication provided insights about the implemented key exchange protocols, the encryption and integrity protection, as well as the internal mechanisms for providing the solution's functionality. On server side, the inter-process communication between all involved components was also inspected and evaluated for possible attack scenarios. To certify the protection against attacks via incoming data paths, a special focus was laid on interfaces handling data that originated from components outside of the BlackBerry Enterprise Solution. Other in-depth inspections were focused, for example, on the effectiveness of the remote administration security of BlackBerry smartphones, their application restriction system and the abilities of third-party applications. The communication of the BlackBerry smartphone with the BlackBerry Infrastructure was inspected closely to verify the data exchanged and to check the protection against network attacks. Additionally, the Bluetooth[1] and USB interfaces of the BlackBerry smartphone were inspected for the effectiveness of the applied security mechanisms.

Other aspects of EAL3 that are not related to the implementation, such as the examination of the development process and the lifecycle of the product, were not considered during the analysis.

[1] See also white paper "Fraunhofer SIT Analysis of BlackBerry Bluetooth Security" at http://www.blackberry.com/security/

2.4 Protection Goals

By determining protection goals for the BlackBerry Enterprise Solution, a list of requirements regarding the BlackBerry Enterprise Solution's security level was created. In each of the three projects concerning BlackBerry communication, the BlackBerry Enterprise Server and BlackBerry smartphone, detailed protection goals have been defined and evaluated. All of these goals were considered mandatory. The following list provides a summarized overview of the goals considered for the certification of the BlackBerry Enterprise Solution. The certified BlackBerry configuration described in section 3.2 has achieved these goals during Fraunhofer Institute SIT Testlab's analysis. All protection goals have been inspected by extensive hands-on tests with knowledge of the underlying design documentation. Additionally, the overall impact of observed functionality for users and administrators was considered regarding violations of protection goals.

The following sections give a brief and summarizing overview of the protection goals that have been defined during the three projects regarding BlackBerry communication, the BlackBerry Enterprise Server and BlackBerry smartphone.

2.4.1 Authenticity

Communication – The complete BlackBerry Enterprise Solution architecture is based on interaction between components using application-driven, transport-driven and management-driven interfaces. Hence, the complete BlackBerry Enterprise Solution architecture is required to use authentication mechanisms to prevent undesired communication to distrusted parties, and to enable a trust relationship between communication counterparts.

Mutual Authentication – Within the BlackBerry Enterprise Solution, all entities participating in the communication process have to prove their identity before any exchange of confidential data starts. The authentication procedures have to be considered as essential in general, since permissions and role mapping are typically built on top of authentication procedures. Their implementation therefore has to be carried out very accurately. Wherever confidential data is transmitted in both directions, it has to be ensured mutually that the counterpart is the party it claims to be. Mutual authentication requires all communication parties involved to prove their identity to each other before starting the exchange of confidential data. Mutual authentication avoids that one of the two parties can get replaced by an attacker.

Trust Relation – Besides an initial mutual authentication of the components upon their first connection, subsequent communication attempts can be authenticated with reduced processing effort. Techniques providing this are known as session management for short-term usage, or trust relationship management for long-term usage. Regardless of how long an authentication context is intended to remain valid, whether it will be stored temporarily or persistently, there must not be any vulnerability in the accordant implementation that would allow it to be broken with appropriate resources.

BlackBerry Enterprise Server Components – Since the BlackBerry Enterprise Server is designed to maintain components on different hosts, these components have to prove their identity to each other before any confidential information is transferred. If any confidential data has to be transmitted in either direction, it has to be ensured mutually that the counterpart is the party it claims to be. In the case that this proof is not possible at the protocol level, the authenticity of communication has to be achieved on a different level, making it impossible that a certain unauthorized user or service is able to derogate the communication by impersonation of other BlackBerry Enterprise Server components.

BlackBerry Infrastructure Interaction – The authenticity of the communication originated by the BlackBerry Enterprise Server has to be ensured. The authentication secret (SRP Authentication Key) has to be securely stored at the BlackBerry Enterprise Server and any interface to obtain this authentication secret has to be protected.

The authenticity of the BlackBerry smartphone to BlackBerry Infrastructure communication originated by the BlackBerry smartphone and directed to the BlackBerry smartphone must be ensured as well. As a result, the registration of the smartphone at the BlackBerry Infrastructure has to be performed using state-of-the-art methods in which the authenticity of each entity has to be proven before any further activity is performed. The BlackBerry Enterprise Server and the BlackBerry smartphone have to ensure that they are communicating with the authentic BlackBerry Infrastructure.

BlackBerry Desktop Manager Interaction – All components of the overall system have to prove their identity before any confidential information is transferred to and from the BlackBerry Desktop Manager. If any confidential data has to be transmitted in either direction, it has to be ensured mutually that the counterpart is the party it claims to be.

Trustworthy User Management – The user management applied and implemented by the BlackBerry Enterprise Server has to be a solid basis for its processes and policies. The server has to be able to limit access to applications and resources, user authentication administration, access rights, access restrictions, account profiles, passwords and (if needed) other attributes supportive of users' roles or profiles. Trustworthy user management includes the BlackBerry smartphone user-to-mailbox mapping, whose authenticity has to be assured from the earliest stage of assignment.

Routing Information – The BlackBerry Router component of the BlackBerry Enterprise Server manages all routing of data to BlackBerry smartphones, and vice versa, in terms of selecting the appropriate communication path (via internal network to USB interface, or via external network to cellular network interface). The authenticity of the routing trigger data is therefore of prime importance for the working of the system as a whole, since it is possible to route data to other entities as well. Therefore, the authenticity of routing trigger data has to be protected.

BlackBerry Smartphone – It is required to prevent or detect undesired smartphone communication to or from distrusted parties by authentication and to enable a trust relationship between communication counterparts. This includes that communication on every interface or access to information or resources has only to be permitted if the digital identity of the counterpart has been proven using authentication mechanisms.

Third-Party Applications – Trusted applications are allowed to perform special actions or use controlled APIs, and these are therefore labeled with some sort of marker. Considering the characteristic of this marker, it has to be ensured that only authorized and trustworthy entities may generate the markers to applications, and that the affiliation between an application and its marker could not be dissolved.

2.4.2 Access Control

The BlackBerry Enterprise Solution has to protect front-end data, back-end data and system resources by implementing access control restrictions. These restrictions should limit the actions performed by users, administrators or counterparts, the resources they have access to and which functions they are allowed to perform.

The access control scheme should protect the solution against unauthorized data-viewing, -modification or -copying. Additionally, it should limit malicious code execution or unauthorized actions of an attacker exploiting components.

Data Flow – A reliable access control considering data flow must validate if two communication parties are allowed, in general, to communicate with each other. This covers all phases of communication: connecting, disconnecting, sending and requesting data.

Flow Control – Whenever a data path is to be established, it has to be ensured by access control that the participating parties are allowed to join this path.

BlackBerry Infrastructure Access Protection – Supported by the authentication procedure, access control has to be able to reliably protect the BlackBerry Infrastructure against unauthorized access.

User Data Protection – Access to personal user data, for example, emails, calendar entries, etc., has to be limited to authorized users.

User-specific Data Protection – The BlackBerry Enterprise Server also manages user-specific data, for example, usernames or authentication credentials to external services. Unauthorized access to any user-specific data using the BlackBerry Enterprise Server as a sort of tunnel – bypassing the security perimeters – has to be prevented.

Server-specific Data Protection – BlackBerry Enterprise Server-specific data, including data used only within the server or any other confidential data utilized with external entities by this server has to be protected against unauthorized access.

Server Components Access Control – The privileges or permissions have to determine specific access rights, such as to "read from", "write to" or "execute" a component to enforce privilege separation. This requires software mechanisms which limit the access to certain services or network ports of each server component, controlling both inbound and outbound traffic. The access control may be determined by a certain user or a group of users.

Controlled Management Access – The access to any management consoles (i.e. BlackBerry Manager) has to be limited to authorized corporate entities only.

Application-Specific Data – The BlackBerry smartphone provides a multitasking operating system, which enables it to exchange data such as application data, user data and user-specific data between the processes executed. Any unauthorized access, unauthorized information disclosure or unauthorized modification of any data in smartphone inter-process communication has to be prevented.

User-defined Restrictions on Application Level – In case the user is able to modify defined restrictions on applications, the user must only be able to strengthen the security level of restrictions but should not be able to lessen them below the level defined by the administrative IT policy. Any unauthorized modification of user-defined restrictions at the application level has to be prevented.

Data Flow Restriction on BlackBerry Smartphone – The data flow restriction is based on the restriction of communication interfaces like PIN messages, SMS, MMS, WAP, phone, browser, voice activated dialing, and Bluetooth. Any circumvention of communication interface restrictions has to be prevented.

Software Upload – The software upload process has to ensure that no unauthorized entity has the permission to upload or install applications.

Software Download – The software backup process has to ensure that no unauthorized entity has the permission to download or backup smartphone-specific data, user-specific data, user data or any application.

Software Modification – The software update process has to ensure that any unauthorized modification of the operating system and installed applications has to be prevented or detected.

2.4.3 Confidentiality

The meaning of confidentiality of data is essential in any private, business or governmental context. Regarding the BlackBerry Enterprise Solution, it must not be possible for any third party to observe communication on any interface or process executed on the server or smartphone side. In the scope of this evaluation, confidentiality is not limited to the protection of exchanged data at the application level or network level. Additionally, confidentiality has to be guaranteed for data transmissions between all involved components as well as

for runtime and stored data within the BlackBerry Enterprise Server and BlackBerry smartphone.

Proper Use of Cryptographic Algorithms – The cryptographic algorithms used for key establishment, key generation, encryption and other security mechanisms have to be implemented properly and have to conform to the corresponding standard. The same applies for the cryptographic API on the BlackBerry smartphone. That means no similar implementations or proprietary "optimizations" are allowed in order to achieve this protection goal.

Secure Lifecycle Management of Shared Secrets or Keys – The whole lifecycle of shared secrets or keys has to be ensured by reliable key exchange mechanisms, which have to be triggered by a maximum key lifetime (time or amount of data encrypted with this key) and robust key replacement mechanisms, which have to be robust concerning data modification or information disclosure during the key exchange process.

Secure Key and Smartphone Password Storage – The security of secret tokens such as keys, shared secrets or the BlackBerry smartphone password has to be ensured by reliably encrypted key stores and must not be accessible to attackers without very high costs and effort.

No Hidden Functionality or Backdoors – There must not be any possibility for RIM or any other third party to read application data transmitted or stored by BlackBerry smartphone users in any case. This protection goal has to be seen as independent from the use of additional encryption like S/MIME or PGP.

No Key Escrow – It has to be ensured that RIM or any other third party does not have access to any secrets that will be shared between the BlackBerry smartphone and the BlackBerry Enterprise Server.

Confidential Server Component Data Exchange – In case server components are placed on separate nodes, the network data confidentiality has to be ensured, for example, by component-to-component data encryption, or other appropriate mechanisms.

Secure Data Handling – Secure data handling is comprised of methods for storage, retrieval and disposal of data. The server's data handling is required to treat server-side access data, cached data, log data, runtime data and temporal data with accuracy — the data must not be accessible by unauthorized persons. The BlackBerry smartphone data handling has to treat smartphone-side access data, cached data, log data, runtime data and temporal data with accuracy — the data must not be accessible by unauthorized persons. Considering temporal, runtime and log data, it should not be possible for any unauthorized person to gain knowledge about the original data on the basis of the provoking (temporal, runtime or log) data.

Secure Data Storage – Data has to be stored securely on the BlackBerry smartphone. This data includes user data, smartphone-specific data, and configuration data. The data storage mechanism on the smartphone has to perform both confidential storage of information within the data categories

mentioned before, which has to consider key management, and the secure deletion of freed physical memory.

2.4.4 Integrity

Integrity testing for all data transmitted is inevitable as a protection against manipulation of the communication and their counterparts with respect to the components considered. Because the transmission happens through public data networks (GPRS and Internet) manipulation of any data transferred via the utilized interfaces can not be prevented. For this reason, it has to be assured that manipulated data on any interface will be detected. Integrity has not only to be considered as a protection against transmission errors, but also against willful manipulation. Since an attacker can manipulate data at any transmission layer, integrity has to be guaranteed at all interface layers.

Data Flow – It must not be possible to change or duplicate messages in transit without this getting noticed and reported by the system.

Communication Path – It must not be possible to bypass, deflect or replace messages in transit from one data path to another without this getting noticed and reported by the system.

Message Data – The transmission of messages through the BlackBerry Infrastructure must not enable any third party, including the operators of the BlackBerry Infrastructure, to change encrypted message data without this being noticed by the receiving communication endpoint.

Configuration Data – The integrity has to be verified for the BlackBerry smartphone configuration as well as for configuration affecting security. Once an IT policy has been transmitted to the BlackBerry smartphone, it has to be ensured that this policy was not altered during transmission.

User-specific Content – It must not be possible for unauthorized persons or applications to alter any user-specific settings or content such as email messages, contact and calendar information without a notification presented to the user.

Integrity of Server Communication – In case of operating a BlackBerry domain or having the BlackBerry Enterprise Server components deployed on different hosts for other reasons, the integrity of data transmitted between these components is of special interest. An integrity protection must prohibit any negative impact on security, for example, by malformed, dropped or duplicated protocol messages.

2.4.5 End-to-End Security

The isolated fulfillment of the aforementioned protection goals will not guarantee end-to-end security automatically. This is because end-to-end security is based on authenticity, confidentiality, access control and integrity, but is actually more than these protection goals, since the complete composition of the communication path or entity interaction is considered one

virtual channel. From the user's perspective, it is of importance that there is no place between the Microsoft Exchange Server and the BlackBerry smartphone, or the BlackBerry Enterprise Server and the BlackBerry smartphone, where messages can be read or changed by an attacker.

To achieve real end-to-end-security, the BlackBerry Enterprise Solution must provide sufficient security at all of its interface layers.

From the security analysis' point of view, the communication ends at the Microsoft Exchange Server and BlackBerry smartphone, respectively. Therefore, this protection goal is reached if the communication is protected between the BlackBerry smartphone and the Microsoft Exchange Server.

2.4.6 Availability

BlackBerry Infrastructure – The availability of this component is of prime importance for the performance of the system as a whole. Thus, attacks on its availability must not be possible with lower effort than targeted on other Internet based components. In case of loss of connection, or in case of a connection becoming inoperative, it must be established again automatically.

MAPI Interface – In case of loss of the connection between the BlackBerry Enterprise Server and the Microsoft Exchange Server MAPI interface, or in case this connection becomes inoperative, the connection must be established again automatically.

Administration interface – The server's administrative interface must always be accessible to administrators via the management console (i.e., BlackBerry Manager). This especially means that there must not be any possibility for attackers to make this administration tool inaccessible.

Resistance – The BlackBerry smartphone must not enter any state where the user cannot access the graphical user interface. Applications rendered inoperative must not block the whole BlackBerry smartphone at once. Even when used aggressively by users or applications, the smartphone should stay listening on its communication interfaces.

Managing of System Resources – There has to be a basic protection against disproportional usage of system resources (CPU load, RAM capacity and storage size) to prevent BlackBerry components from being blocked by willful resource exhaustion.

Network Interface – There should be no possibility for an attacker to stop the BlackBerry smartphone from accessing the network interface at the software level.

Medium Robustness against Denial-of-Service Attacks – The BlackBerry Enterprise Solution must provide a basic protection against Denial-of-Service attacks originated by single attackers.

2.4.7 Reliability

Since data to be processed by the BlackBerry Enterprise Solution could be corrupted due to transmission errors or intentional actions, the software must be error proof in all cases. Examples of willful corrupted data are email attachments containing malformed image file headers or decompression bombs. In both cases, non-reliable data processing would cause the software to become vulnerable to Denial-of-Service or buffer overflow attacks.

Reliable Security Enforcement – The security architecture of the BlackBerry Enterprise Solution incorporates remotely assignable policy rules to the BlackBerry smartphone. These policies have to be enforced on the smartphone by effective security middleware mechanisms. In particular, the restrictions applied on the smartphones for all of its interfaces must always comply with the administrative settings.

2.4.8 Ease of Use Security

Secure handling of the BlackBerry Enterprise Solution should be easy, to avoid dangerous user actions by user mistakes. As the software is designated to deal with personal and confidential data, there is the need for clear and comprehensible user guidance for all security-related settings and work flows. This aims to provide ease of use for users while excluding the risk of security threats to the information handled by the system at the same time.

Visibility of Communication Security – The system state of security should be easily apparent to its operators and users. They should be able to distinguish between normal operations and any security violations at a glance.

Configurability of Communication Security – Any consequences or security dependencies caused by changes of settings relevant to communication security have to be easily apparent to its operators and users. The information displayed has to reflect the possible loss of security that a user has to take into account.

Dialogs – With regard to security, ease of use in practice depends mainly on the quality of application dialogs. A fitting graphical user interface has to assist a user with security relevant configuration tasks by giving advice or providing information on possible security implications of specific settings.

Precise IT Policy rules – The descriptions of IT policy rules have to clearly indicate their effect and should not leave any room for interpretation.

Deterministic Behavior – The behavior of smartphone applications and server services should always be deterministic in terms of the same functionality always reproducing the same results.

No Stumbling Blocks – The server's management console (i.e., BlackBerry Manager) must not provide any options that can mislead administrators to accidentally perform actions that have a negative impact on security.

2.5 Assumptions and Limitations

The items described in the following are building the foundation of assumptions and limitations for the security analysis. All considerations and basic conditions denoted below were assumed guaranteed and therefore were not verified or put into question during the analysis.

BlackBerry Smartphone to BlackBerry Infrastructure Assignment – Since several entities of the BlackBerry Infrastructure coexist (several operational and at least one development BlackBerry Infrastructure that was used), there is a mechanism which defines which smartphone is served by which BlackBerry Infrastructure. The evaluators presupposed that the assignment of a BlackBerry smartphone to one BlackBerry Infrastructure and the operation with that entity has no influence on the security characteristics.

Physical and Side Channel Attacks on BlackBerry Smartphone – The housing of the BlackBerry smartphone was specified to remain closed. The evaluators did not attempt any attacks requiring the housing to be opened. Physical attacks to the BlackBerry smartphone were out of scope. This exclusion also refers to hardware interfaces on the PCB for developers such as JTAG and more specialized attacks threatening discrete components on the PCB, such as CPU, RAM and ROM, and physical side-channel attacks measuring electromagnetic radiation or power consumption.

Implementation – The evaluation presupposed that a security guideline is provided to the programmers of BlackBerry components, processes and interfaces to avoid new vulnerabilities creeping in while implementing new functionality.

External Mechanisms – External mechanisms and services used by the BlackBerry Enterprise Solution were excluded from the analysis. External mechanisms refer to mechanisms vendors other than RIM are responsible for, or mechanisms that rely on standard transport or application protocols. External services refer to communication counterparts for BlackBerry Enterprise Server services such as the BlackBerry Collaboration Service or the BlackBerry® Mobile Data System Services.

Deployment – The delivery status of the BlackBerry smartphones is important with regard to trustworthy security. The security analysis is based on the assumption that the hardware and software of BlackBerry smartphones are not manipulated by third parties before the roll out to the BlackBerry smartphone users.

Physical Security – The physical security of the BlackBerry Enterprise Server as well as the BlackBerry Infrastructure was assumed guaranteed. In this context, physical security is denoted for example by access for third parties to server and infrastructure components. A third party is defined as the physical access group of potential persons that are not directly involved in maintenance or usage of the server and infrastructure. It was furthermore assumed that all BlackBerry Enterprise Server components are running locally on systems attended by local system administrators. The administrators are assumed to take responsibility in

terms of security aspects and trustfulness. The administrators also have to make sure that physical access to the server is granted to authorized staff only.

Qualified Staff – All work on components of the BlackBerry Enterprise Solution, including the management and the implementation of technical measures, is assumed to be carried out by skilled experts. Additionally, the staff operating the BlackBerry Enterprise Server and the BlackBerry Infrastructure, including their subsystems, has to be trained for the duty of secrecy. It is also assumed that there is at least one administrator responsible for configuration and maintenance of the BlackBerry Enterprise Server.

3 Certified Deployment

3.1 Certified Component Versions

The following list presents the versions of the BlackBerry Enterprise Solution components fulfilling the certification requirements. This fulfillment refers to the certified configuration presented in section 3.2 and residual risks presented in section 3.3.

Based on the short lifecycle of the inspected product and the required effort for the evaluation, it was inevitable to consider product updates during the term of the analysis. These product updates included further improvements recommended by the IT Security Testlab to meet the certification requirements, and in some cases also introduced new hardware or software functionality that was beyond the initial evaluation focus. For this reason, the version of the initial functionality tested is listed for reference. Thus, all statements regarding the certified versions are limited to the functionality, interfaces and processes of the initially-deployed BlackBerry Enterprise Solution component versions.

The certified versions are compliant with the protection goals (see section 2.4) considering the functionality of the initially-deployed versions.

BlackBerry® Enterprise Server for Microsoft Exchange

Certified version:
v4.1.6 (bundle 60)

Initially deployed version during analysis:
v4.1.2 (bundle 23)

BlackBerry Smartphone

Certified version:
BlackBerry® Pearl™ 8110 smartphone (EDGE),
Firmware: v4.3.0.104 (Platform 2.6.0.59) and
Cryptographic Kernel: v3.8.5.11c

Initially-deployed version during analysis:
BlackBerry® 8700 smartphone (EDGE),
Firmware: v4.2.1.37 (Platform 2.3.0.33) and
Cryptographic Kernel: v3.8.4.34

3.2 Certified Configuration

Because of the wide range of configuration options within the BlackBerry Enterprise Solution by dint of IT policies, component configurations and their deployment, the certificate is limited to the following configuration containing IT policy options, component deployment and configuration options.

All subsequent presented limitations and configuration options are required to meet the security level defined by the protection goals. Therefore, this section summarizes the certified configuration for this evaluation. Applying this configuration is mandatory to achieve results comparable to the outcome of this evaluation.

Unless stated otherwise, the presented configuration option has to be applied using the BlackBerry Manager.

AES Deployment – In the certified configuration, the deployment of the BlackBerry Enterprise Solution is limited to AES encryption mode to meet the security goals of the certification context.

Therefore, the following configuration changes have to be arranged on the basis of default configuration to be inline with the certified configuration:

- Selection of "AES" in the Server Configuration tab "General / Security / Encryption Algorithm"
- Selection of "True" in the IT policy item "Security Policy Group / Disable 3DES Transport Crypto"

Disabling Messaging Server Storage of Master Encryption Keys – The storage of the BlackBerry smartphone Master Encryption Keys in the user's mailbox has to be disabled to be inline with the certified configuration. The resulting loss of functionality (e.g., the inability to perform "Wired Activation") within the BlackBerry Enterprise Solution due to this configuration change is rated from the security analysis perspective as an intentional and mandatory consequence.

The configuration change is supported and described by RIM in the knowledge base article [KB_MEKStrorage], listed in the reference section of this document.

Secure network configuration of BlackBerry Attachment Server – The separation of the BlackBerry Attachment Server from other BlackBerry Enterprise Server components has to be taken into consideration to match the certified configuration.

The BlackBerry Attachment Server has to be separated from other BlackBerry Enterprise Server components and has to run in a firewalled network according the Technical Note "Placing the BlackBerry Enterprise Solution in a Segmented Network Version 4.0 and 4.1" [WP_SegmentedNetwork_4.0].

Exclusion of BlackBerry roles – BlackBerry administrative roles must not be used, or the roles applied must only consist of administrators assigned to the "Security Administrator" role to be inline with the certified configuration.

For BlackBerry Enterprise Server administration the roles are intended to group trusted administrators according to the scope of their administrative responsibility. These roles are: "Security administrator", "Enterprise administrator", "Device administrator", "Senior help desk administrator", "Junior help desk administrator" and their audit role counterparts such as

"Audit Security administrator" and so on (see the knowledge base article [KB_RoleBasedAdministration]).

Definition and Establishment of Corporate PIN-to-PIN Master Key – The certified configuration requires the generation and establishment of an organization-specific PIN-to-PIN Master Key, which is used to encrypt the communication between BlackBerry smartphones when using PIN messages. This key has to be different from the default PIN-to-PIN Master Key that is used without further configuration after BlackBerry Enterprise Server installation. As this newly created key is unique to each BlackBerry corporate environment, it is called the corporate PIN-to-PIN Master Key within this document.

The process of generating and establishing a corporate PIN-to-PIN Master Key is given in the documentation "Administration Guide BlackBerry Enterprise Server for Microsoft Exchange Version 4.1 Service Pack 6" [WP_AdminGuide_4.1.6] in section "Generating organization-specific encryption keys for PIN-to-PIN message encryption".

Software Configuration with Application White Listing – The certified configuration mandatorily requires white listing of allowed applications to be installable on BlackBerry smartphones.

Application white listing has to be configured by setting the default application setting in the Software Configuration feature of the BlackBerry Enterprise Server to "disallowed" as described in the knowledge base article [KB_SoftwareConfiguration].

Usage of APN that prevents direct Smartphone Access via Network – The certified configuration assumes the usage of an APN that prevents inbound traffic to all BlackBerry smartphones other than data sent from the used BlackBerry Infrastructure. This includes communication that originates from the Internet as well as incoming data from other smartphones on the same wireless network.

The user's mobile operator is in charge of this common APN configuration.

Protection of Intranet Services – Outgoing connections from the BlackBerry MDS Connection Service into the corporate intranet have to be limited at the network layer to dedicated services to be inline with the certified configuration.

Restrict Access to internal BlackBerry Enterprise Server Components' Interfaces – The certified configuration requires intranet access protection of the MDS Service web management interface, MDS Connection Service web management interface and the WAPPush interface to prevent unprivileged access. Firewalls must only allow specific remote workstations to access the respective web interfaces. The loss of functionality is an intentional and mandatory result to achieve the certification requirements.

Additional Mandatory Default IT Policy Changes – Compared to the default IT policy, the following IT policy rules have to be set to be inline with the certification context:

- Selection of "True" in the IT policy item "Device-Only Items / Password Required"
- Modification to "6" in the IT policy item "Device-Only Items / Minimum Password Length"
- Selection of "False" in the IT policy item "Device-Only Items / User can disable Password"
- Modification to "5" in the IT policy item "Device-Only Items / Maximum Security Timeout"
- Selection of "True" in the IT policy item "Device-Only Items / Enable Long-Term Logout"
- Selection of "At least 1 alpha, 1 numeric character" in the IT policy item "Device-Only Items / Password Pattern Checks"
- Selection of "True" in the IT policy item "Security Policy Group / Require Secure APB Message"
- Selection of "Strong" in the IT policy item "Security Policy Group / Content Protection Strength"

3.3 Residual Risks

Besides protection against known attacks, the limitation of access privileges within the operating system is a feasible method to protect software based systems. In case of vulnerabilities such as arbitrary code execution, this limitation of privileges can reduce the impact for the overall system, since the injected code is permitted only to perform actions that are granted to the exploited component. This is a general security aspect that applies to any software in security relevant environments and is not specific to the way the BlackBerry Enterprise Solution is designed.

The presented configuration provides strong protection against known attack mechanisms. However, the BlackBerry Enterprise Server configuration for the host operating system do not extend to a setup that is designed specifically to limit the impact of an attack that results in arbitrary code execution on a BlackBerry Enterprise Server component. This additional protection can be provided by the operating system with tailored privilege settings for all involved components and services. Such mechanisms would reduce the risks for the corporate data and have to be considered state-of-the-art for security relevant environments.

In contrast, all BlackBerry Enterprise Server components and services are running with extensive permissions after the installation on the test system. These permissions allow read and write access to the Microsoft Exchange Mail Storage, the BlackBerry Configuration Database and local administrative access to the hosting Microsoft Windows operating system.

In detail, the permissions of the components BlackBerry Alert, BlackBerry Collaboration Service, BlackBerry Controller, BlackBerry Dispatcher, BlackBerry MDS Connection Service, BlackBerry MDS Integration Service, BlackBerry Policy Service, BlackBerry Router and BlackBerry Synchronization Service are running with the privileges of the BlackBerry Server Service account. This account

includes full access to the mailboxes on the affiliated Microsoft Exchange Server as well as full access to the BlackBerry Configuration Database. This circumstance authorizes all BlackBerry Enterprise Server components and services mentioned above to access all sensitive and private data stored in these sources.

Additionally, the BlackBerry Attachment Service is executed with permissions of the local system account (NT_AUTHORITY\SYSTEM). This account includes more privileges than owned by a local administrator.

The deficient granular assignment of permissions could enable an attacker to fully control the information resources and the hosting system, if he manages to take over one of the mentioned BlackBerry Enterprise Server components or services.

Consequently, the evaluation object in the presented certified configuration does not meet all protection goals postulated during the security analysis regarding achievable security. As there is no BlackBerry Enterprise Server configuration that is designed specifically to handle the above mentioned context, the following risks remain:

a) Residual risk regarding the Microsoft Windows installation hosting the BlackBerry Enterprise Server – In case of an attack resulting in arbitrary code execution on a BlackBerry Enterprise Server component a total loss of confidentiality, integrity and privacy of the hosting Microsoft Windows installation can occur. In this case, all data stored on that particular server and on all other Windows installations accessible with stored credentials used somewhere on the BlackBerry Enterprise Server are affected too. Additionally, total loss of confidentiality is imminent regarding unencrypted HTTP connections or connections using the BlackBerry MDS Connection Service as proxy.

b) Residual risk regarding mailboxes of connected Microsoft Exchange server – Total loss of confidentiality, integrity and privacy of all data within all mailboxes of the connected Microsoft Exchange server in case of an attack resulting in arbitrary code execution on one of the following BlackBerry Enterprise Server components: BlackBerry Messaging Agent, BlackBerry Collaboration Service, BlackBerry Dispatcher, BlackBerry MDS Connection Service, BlackBerry MDS Integration Service, BlackBerry Policy Service, BlackBerry Router or BlackBerry Synchronization Service.

c) Residual risk regarding the Configuration Database – Total loss of confidentiality, integrity and privacy of all data within the Configuration Database in case of an attack resulting in arbitrary code execution on one of the following BlackBerry Enterprise Server components: BlackBerry Messaging Agent, BlackBerry Collaboration Service, BlackBerry Dispatcher, BlackBerry MDS Connection Service, BlackBerry MDS Integration Service, BlackBerry Policy Service, BlackBerry Router or BlackBerry Synchronization Service.

d) Residual risk regarding transmitted data within the BlackBerry Enterprise Solution – Total loss of authenticity, confidentiality, integrity and

privacy of transmitted data within the BlackBerry Enterprise Solution (from BlackBerry Enterprise Server to BlackBerry smartphone and vice versa) in case of a compromised Configuration Database (in the wake of residual risk item (c)).

4 Certificate Result Statement

The IT Security Testlab of the Fraunhofer Institute for Secure Information Technology SIT certifies that the BlackBerry Enterprise Solution for Microsoft Exchange by

Research in Motion Limited
295 Phillip Street, Waterloo, Ontario, Canada N2L 3W8

has passed the security analysis. The certificate is based on the functionality, configuration and installation limitations described in this document.

In the certified configuration, the tested BlackBerry Enterprise Solution achieves the protection goals set by Fraunhofer Institute SIT. Additionally, statements about important security properties of the product are based on the evaluation results.

The recommended AES-256 implementation is compliant to the standard, which provides high security encryption. The transmission of information via the BlackBerry Infrastructure is considered to be secure, since the encryption used for messages transmitted over the Internet, the wireless interfaces or wireless service provider's network could not be broken within appropriate time and resources and the communication secrets remain unknown to any third party, including RIM. The security is therefore based on the complexity of the cryptographic algorithm. Considering current scientific knowledge and available computing power, the protection provided by the standards-compliant AES usage within the BlackBerry Enterprise Solution is deemed secure.

Based on approved secure key establishment and key exchange protocols the confidentiality and integrity of pushed content is provided and can not be eavesdropped on by any party inside the communication channel.

In our analysis of the BlackBerry Enterprise Solution, we did not find any evidence for the existence of a master key, back door or a function that would allow RIM to read customer’s emails.

The evaluation of the BlackBerry Enterprise Server did not unveil any functionality that could be used by RIM for accessing information localized on the BlackBerry Enterprise Server, on other computers or via network systems connected to or accessible by the BlackBerry Enterprise Server.

With the described configuration, the BlackBerry smartphones offer state-of-the-art protection against software level attacks. The remote smartphone management functionality offers secure administration of BlackBerry smartphones and the configurable smartphone restrictions could not be circumvented in the certified configuration.

The BlackBerry communication provides end-to-end security for the evaluated interactions and services between BlackBerry smartphones and the BlackBerry Enterprise Server. For the residual risks on server side, refer to section 3.3.

Product:	BlackBerry Enterprise Solution for Microsoft Exchange
Certified Version[2]:	BlackBerry Enterprise Server v4.1.6 (bundle 60) BlackBerry® Pearl™ 8110 smartphone (EDGE), Firmware: v4.3.0.104 (Platform 2.6.0.59) and Cryptographic Kernel: v3.8.5.11c
Date:	2008-11-24
Certificate no.:	06-104302
Certificate validity:	until December 2010

[2] The certified versions are compliant with the protection goals (see section 2.4) considering the functionality of the initially deployed versions (see section 3.1).

5 Fraunhofer Institute SIT

The Fraunhofer-Gesellschaft is the leading organization for applied research in Germany undertaking research of direct utility to private and public enterprise and of wide benefit to society. Its services are solicited by customers and contractual partners in industry, the service sector and public administration. The Fraunhofer Information- and Communication Technology Group within the Fraunhofer-Gesellschaft represents the biggest, coordinated capacity in the field of applied research in informatics within Europe.

The goal of Fraunhofer Institute SIT – as leading member in terms of IT security in the Fraunhofer Information- and Communication Technology Group – is to provide scalable IT security in conformance to market needs. Building on a foundation of excellent strategic scientific research, the Institute improves IT security generally and develops new security technologies and applications.

Apart from these aspects the Institute examines the security characteristics of software or software-based systems and services in its IT Security Testlab. The Testlab performs individual and application orientated security tests of IT systems to effectively identify security gaps and reliably and meaningfully inform about security characteristics of products and services.

If a product demonstrates sufficient security characteristics regarding the stated security requirements, the Fraunhofer Institute SIT assigns a qualified, product specific certificate. This certificate and the associated documentation are the transparent and comprehensible representation of the test results obtained.

5.1 Evaluation Principles

The basic evaluation principle Fraunhofer Institute's IT Security Testlab postulates that an IT system with sufficient security characteristics does not exhibit relevant security flaws in its typical application and deployment context. To ensure the evaluation all well-known security gaps are considered that endanger the general protection goals of the integrity, privacy, availability and non-repudiation.

Vulnerabilities in distinct parts of a product may seem a minor issue when considered separately, but any combination of these minor issues can facilitate a major attack. Standard tests are unable to uncover such hidden dangers. Therefore the actual security of a product cannot be evaluated by block operation determining isolated security mechanisms. At Fraunhofer Institute's IT Security Testlab trained experts examine systems with knowledge of common software-vulnerabilities and state-of-the-art attack techniques and tools. Consequently the components and interfaces of a system are systematically studied. Using this inventory, realistic scenarios for potential attacks in typical deployment situations are developed. These scenarios serve as the basis of targeted tests.

The evaluation depth is of crucial importance for the statements about the security characteristics of a product or a service. In order to ensure reliable and sufficiently qualified statements about a system, the expenditure and time of an evaluation at Fraunhofer Institute SIT's IT Security Testlab are allocated abundantly, appropriate to the security need of the evaluation object within its application and deployment context. The depth of the examination of the components depends on the expected impact and on threats outlined as well.

The Testlab offers on the one hand the investigations to be accomplished in a black box procedure, for example without knowledge of the internal structure of the evaluation object. Specifications of relevant interfaces and security characteristics hereby serve more effective examination of attack vectors. On the other hand a white box procedure can be performed in critical areas of application; proven due to the higher security statements in the Fraunhofer Institute SIT-Certificate separately.

Security analyses and certificates of Fraunhofer Institute SIT are to be understood as a complement stage to the formal certificates, like the Common Criteria for Information Technology Security (CC) certifying framework. The overall proceeding of the IT Security Testlab is particularly suitable for situations, in which no CC protection profile for the respective context exists. Even if a protection profile is present, the evaluation could be appropriate, if the protection profile does not match sufficiently with the special application area of the product or service.

5.2 Evaluation Process Pattern

The evaluation process pattern is divided in 4 phases. The first phase provides an overview of the TOE architecture and involved components by analyzing all parts, its communication protocols and corresponding interfaces. The goal of this phase is to identify potential weaknesses and assets that have to be protected.

In the second phase potential threats to these assets are described. Together with the consideration of current protection technologies the results will build the basis for the definition of security requirements. This is done to check the evaluation object against the requirements and to provide a basis for the stated security conclusions. From the security requirements general and specific risks are determined, resulting in the specification of attack scenarios.

Phase three analyses the security impacts on the evaluation object and its environment by executing the attack scenarios, periodically cycled to include new observations discovered during attacks. To execute the scenarios, automatic and manual tools are used to find and to exploit weaknesses.

Finally phase four concludes the results by summarizing the gathered facts. Additionally suggestions are provided to increase the security for proven weaknesses. To meet the requirements and to receive the certification the evaluation object can go through several re-evaluations which will start again in phase three.

References

[KB_MEKStrorage]	Knowledge Base Article no. 10726 - Turn off messaging server storage of BlackBerry smartphone master encryption keys; http://www.blackberry.com/btsc/search.do?cmd=displayKC&externalId=KB10726
[KB_RoleBasedAdministration]	Knowledge Base Article no. 04889 - What is role based administration; http://www.blackberry.com/btsc/search.do?cmd=displayKC&externalId=KB04889
[KB_SoftwareConfiguration]	Knowledge Base Article no. 05392 - Control and remove third-party software using software configuration; http://www.blackberry.com/btsc/search.do?cmd=displayKC&externalId=KB05392
[WP_AdminGuide_4.1.6]	Administration Guide BlackBerry Enterprise Server for Microsoft Exchange Version 4.1 Service Pack 6; http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/7963/7965/1180408/Administration_Guide.pdf?nodeid=1442745&vernum=0
[WP_SegmentedNetwork_4.0]	Technical Note - Placing the BlackBerry Enterprise Solution in a Segmented Network; Version 4.0 and 4.1; http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Placement_of_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf?nodeid=1265885&vernum=0 Technischer Hinweis - Einbinden der BlackBerry Enterprise Solution in ein segmentiertes Netzwerk; Version: 4.0 und 4.1; http://na.blackberry.com/eng/deliverables/4901/Einbinden_der_BlackBerry_Enterprise_Solution_in_ein_segmentiertes_Netzwerk.pdf

Disclaimer

This document does not warrant or guarantee the accuracy, completeness, or adequacy of the information herein, and this report makes no representations or warranties regarding the security of the BlackBerry Enterprise Solution or forward-looking statements.

Users of this information act at their own risk and are urged to consult independent professional support regarding the deployment of the technology assessed.

Nothing herein shall be construed as a warranty, guarantee or binding commitment on the part of Fraunhofer Institute SIT, nor as any authorization to perform any activities respecting the BlackBerry Enterprise Solution that are not expressly permitted by the applicable RIM licenses and/or end user agreements.

The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties and trademarks of Research In Motion Limited.

Windows and Exchange are registered trademarks of Microsoft Corporation in the United States and other countries.