Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

SICHERHEITSANALYSE - BLACKBERRY MOBILE DATA SERVICE (VERSION1.0, OKTOBER 2004)

Diese Studie wurde von A-SIT im Auftrag des Bundeskanzleramts durchgeführt

Dipl.-Ing. Kurt Dietrich • IAIK • eMail: Kurt.Dietrich@iaik.tugraz.at

Überblick: In diesem Dokument werden die vorhandenen Sicherheitsmechanismen des BlackBerry Mobile Data Service [1] identifiziert und analysiert. Als Basis der Analyse dienen Information aus der Online Dokumentation von BlackBerry [2] sowie Informationen von Mitarbeitern der Mobilkom und der Firma BlackBerry.

Dazu ist die Analyse ist in vier Bereiche unterteilt:

- **Übertragungssicherheit**
  Dieses Kapitel behandelt die Sicherung des Übertragungsweges zwischen Handheld und Firmennetzwerk.
- **Gerätesicherheit**
  Dieser Punkt geht auf spezifische Sicherheitsprobleme mit vertraulichen Daten auf den mobilen BlackBerry Handhelds ein.
- **Applikationssicherheit**
  Behandelt die Frage, ob es dem Benutzer möglich ist, Applikationen am Handheld zu installieren und damit unbewusst eine Sicherheitslücke zu öffnen.
- **Optionale Komponenten**
  Behandelt optionale Softwarekomponenten, die Einfluss auf die Sicherheit des Services haben.

Am Ende des Dokumentes befindet sich eine Zusammenfassung, die einen schnellen Überblick über die Ergebnisse liefert. Um einen unkomplizierten Zugang zu den referenzierten Dokumenten zu ermöglichen, sind die Referenzen (die direkt mit den Dokumenten verlinkt sind) nicht am Ende des Dokumentes sondern am Ende jedes einzelnen Kapitels angehängt. Durch Anklicken des Links, und wenn vorhanden, unter Berücksichtigung der Seiten- bzw. Kapitelangabe lassen sich die informationsgebenden Absätze in den Originaldokumenten leicht wieder finden. Ebenso werden Informationen und Aussagen, die von Dritten stammen (z.B. Mobilkom), als solche gekennzeichnet.

[1] BlackBerry Mobile Data Service, http://www.blackberry.com/products/software/server/mds/index.shtml
[2] BlackBerry online Dokumentation, http://www.blackberry.com/knowledgecenter/public/livelink.exe?func=llworkspace

Inhaltsverzeichnis

Glossar, Abkürzungen

AES	Advanced Encryption Standard – symmetrische Verschlüsselung mit 128, 192 oder 256 Bit effektiver Schlüssellänge (Nachfolger des DES)
API	Application Programming Interface
DES	Data Encryption Standard, symmetrische Verschlüsselung mit 56 Bit effektiver Schlüssellänge
FIPS-140	Federal Information Processing Standard 140: „Security Requirements for Cryptographic Modules“
GPRS	General Packet Radio Service
MAPI	Messaging Application Programming Interface
PDA	Personal Digital Assistant (z.B. BlackBerry)
POP	Post Office Protocol
RIM	Research In Motion
SHA	Secure Hash Algorithm 1
SIM	Subscriber Identity Module
S/MIME	Secure Multi Purpose Mail Extension
SSL, TLS	Secure Socket Layer, Transport Layer Security (TLS bezeichnet die als RFC standardisierte Version von SSL)
USB	Universal Serial Bus
VPN	Virtual Private Network
TripleDES	Triple Data Encryption Standard – DES-Variante mit je nach Verfahren 112 oder 168 Bit effektiver Schlüssellänge

1. Übertragungssicherheit

Der *BlackBerry Enterprise Server* stellt die Schnittstelle zwischen dem Handheld und den sich im Firmennetzwerk befindlichen Mailservern (bzw. dem Firmenintranet) dar [Abb. 1]. Die Verbindung zwischen Handheld und Enterprise Server ist durch eine TripleDES Verschlüsselung abgesichert (in der nächsten Generation soll AES zum Einsatz kommen). Alle übertragenen Daten (Nachrichten und Attachments) werden auf diese Weise gesichert – unabhängig vom verwendeten Transportmedium (GSM, Internet etc.). Nach eigenen Angaben besitzt die Implementierung der Verschlüsselungs-Technologie von BlackBerry am Handheld eine FIPS-140 Zertifizierung [1].

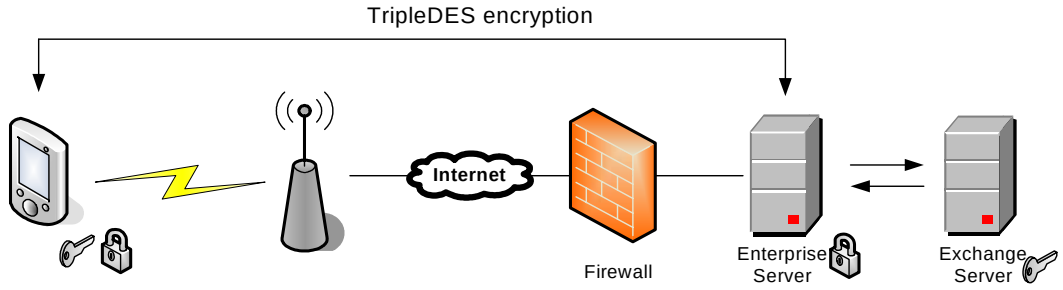

Abbildung 1

Versendet der Benutzer des Handhelds nun eine Nachricht, so geschieht folgendes:

- Die Nachricht wird am Handheld verschlüsselt and an den Enterprise Server geschickt.
- Der Enterprise Server holt den Schlüssel des Besitzers des Handhelds vom Exchange Server und entschlüsselt die Nachricht. Der Schlüssel des Benutzers befindet sich in so genannten „Hidden Folders“ des Benutzers im Exchange Server Account.
- Die Nachricht wird nun unverschlüsselt an den Exchange Server weitergeleitet, welcher wiederum die Nachricht dem betreffenden Empfänger zustellt.

Empfängt ein Benutzer eine Nachricht in die InBox seines Exchange Server Accounts, so wird der Enterprise Server über die MAPI-Connection informiert, dass eine neue Nachricht vorhanden ist. Ob nun die Nachricht an den Handheld weitergeleitet werden soll, kann durch Filter geregelt werden, die der Benutzer definiert bzw. die global definiert sind, (globale Filter-regeln haben Vorrang gegenüber benutzerdefinierten). Die Verbindung zwischen Enterprise Server und Exchange Server kann mittels SSL oder TLS abgesichert werden. Die Nachricht ist somit nur am Enterprise Server und am Exchange Server unverschlüsselt. Entsprechende Maßnahmen zum Schutz dieser Server sind daher notwendig und werden von BlackBerry empfohlen [2].

Versucht sich nun ein Angreifer als ein bestimmter Benutzer auszugeben, um dessen Nachrichten vom Exchange Server abzuholen, so weist ihn der Enterprise Server aufgrund des falschen oder fehlenden Schlüssels zurück.

Durch die verwendete Verschlüsselung ist die Verbindung gegen Abhören gesichert. Bekommt ein Angreifer jedoch ein Gerät in die Hände, so hat er solange Zugriff auf die Daten des Benutzers (Mailbox und Daten am Gerät), bis der Zugang gesperrt wird (siehe Kapitel Datensicherheit). Durch Sicherungsmechanismen bei der GSM Übertragung und durch die Verschlüsselung ist es auch nicht möglich eine bestehende Verbindung zu über-nehmen.

[1] BlackBerry Enterprise Server White Paper, BlackBerry Enterprise Server version 3.6 for Microsoft Exchange Technical White Paper, Kap. “BlackBerry Security / Degree of Security”, Seite 6.

[2] Guidelines for Mobile Data Service security, http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8179/270935/Guidelines_for_Mobile_Data_Service_security.pdf?nodeid=336503&vernum=0

Schlüsselerzeugung und -Austausch

Die Schlüsselerzeugung findet entweder am Desktop PC des Benutzers statt oder (ab Version 4.0) auf einem dafür eingerichteten Server. Bei der Schlüsselerzeugung am PC werden zur Zufallszahlgenerierung Mausbewegungen verwendet. Es werden zwei Kopien des Schlüssels erzeugt: eine Kopie wird an den Handheld gesendet und die andere wird am Exchange Server abgelegt. Der Schlüsselaustausch mit dem PDA ist nur dann erlaubt, wenn sich der PDA in der Cradle des betreffenden PCs befindet[1, 2]. Der Schlüssel kann nicht über andere Kanäle auf den PDA gebracht werden. Außerdem wird nun jeder weitere Informationsaustausch zwischen dem in der Cradle befindlichen PDA und dem Desktop PC mit diesem Schlüssel gesichert.

Es existieren drei Kopien des Schlüssels:

- eine am Exchange Server
- eine am Desktop PC, wo der Schlüssel erzeugt wurde
- eine am BlackBerry PDA

Bei der zweiten Variante wird dem BlackBerry-Benutzer ein Dienst zur Verfügung gestellt, der Schlüssel erzeugt. Der Schlüsselaustausch erfolgt danach drahtlos unter Verwendung von SPEKE (*Simple Password Exponential Key Exchange*) [3]. Dieses Protokoll benötigt ein Passwort, das zur Authentifizierung des Benutzers und zur Erstellung eines Session Keys verwendet wird (genaueres ist unter [3] zu finden). Dieses Passwort darf nicht über die drahtlose Verbindung zum Handheld bzw. Benutzer gesendet werden, sondern muss über einen alternativen Kanal übertragen werden[2]. BlackBerry schlägt vor, den Schlüssel einmal pro Monat zu ändern. Diese Zeitspanne ist auch die Defaulteinstellung der BlackBerry Desktop Software, die einmal im Monat automatisch einen neuen Key erzeugt und austauscht.

[1] BlackBerry Enterprise Server version 2.1 Security White Paper for Microsoft Exchange Seite 6. , Kap. 6. Wireless Link Protection

[2] RIM-Deutschland

[3] Jablon, David P., 2. März 1997 „Strong Password-Only Authenticated Key Exchange“ erhältlich online unter: http://www.integritysciences.com/speke97.html

1 Es existiert kein Mechanismus, der sichergestellt, dass der Schlüssel tatsächlich am PC des Besitzers des Handhelds erstellt wird. Sollte die Schlüsselerzeugung auf einem fremden Rechner erfolgen (z.B. wenn der Benutzer den BlackBerry nicht an seinem eigenen sondern an einen fremden Desktop PC anschließt), so würde eine weitere Kopie des Schlüssels existieren, die womöglich nicht unter der Kontrolle des Benutzers wäre.

2 Die Erzeugung von Zufallszahlen ist für die Erstellung der Schlüssel von größter Wichtigkeit. Uns liegt noch keine Information über die Qualität der Zufallszahlenerzeugung vor. Diese Informationen wurden bei Mobilkom angefragt. Eine endgültige Beurteilung dieser Frage kann erst nach Vorliegen der verfügbaren Informationen getroffen werden, unter Umständen könnte sich eine detaillierte Untersuchung der Mechanismen als empfehlenswert erweisen.

2. Gerätesicherheit

Passwortsicherheit am Mobilgerät

Der BlackBerry ist mit einem Bildschirmschoner versehen, der nach einer definierbaren Zeit den Zugang zum Gerät unterbindet. Dabei werden das Keyboard, das USB Port und das Infrarotport gesperrt. Unterstützung für Bluetooth bieten nur einige wenige BlackBerry Handhelds, die allerdings keinen Zugriff auf das Gerät über Bluetooth erlauben. Der Benutzer kann Passwörter in der Länge von 4 bis 14 Zeichen verwenden. Schwache Passwörter wie „1234“ oder Passwörter aus sich wiederholenden Zeichen wie „bbbbb“ etc. werden vom Gerät nicht akzeptiert. Vom Passwort selbst wird nur der SHA-1 Hash am Gerät gespeichert. Nach zehn hintereinander erfolgten falschen Passworteingaben werden alle benutzerspezifischen Daten gelöscht. Die maximale Anzahl der falschen Eingaben kann durch eine entsprechende IT-Policy geändert werden. Als Mindestlänge können 1 bis 12 Zeichen durch die Policy verlangt werden [4].

Datensicherung

Die Nachrichten und deren Attachments werden im Klartext am Gerät gespeichert. Version 4.0 des BlackBerry Handhelds bietet in Zukunft auch die Möglichkeit, diese Daten lokal zu verschlüsseln [3]. Dabei soll der AES Algorithmus zum Einsatz kommen (mit Schlüssellängen von 128 bis 256 Bit). Eine aus der Ferne initiierbare Löschung der Daten im Falle eines Diebstahles oder Verlustes des Gerätes ist vom Hersteller zwar vorgesehen, kann aber mit entsprechend einfachen Mitteln und Methoden unterbunden werden (z.B. durch Tauschen oder Entfernen der SIM-Karte) und ist daher als wenig effektiv zu betrachten.

Der BlackBerry ist mit einem Bildschirmschoner ausgestattet, der den Zugriff auf die Daten und Applikationen des Gerätes nach einem definierten Intervall unterbindet und nur mit dem richtigen Passwort wieder erlaubt. Zwar schützt dieser Schoner vor Zugriff auf das Gerät und blockiert Verbindungen über Infrarot oder USB nach außen bzw. von außen (über die bestehende GSM/GPRS Verbindung werden nur Daten angenommen, die mit dem entsprechenden 3DES Schlüssel verschlüsselt sind), allerdings besteht kein Schutz gegen einen mechanischen Einbruch in das Gerät. Werden die Hardwarekomponenten (speziell die Speichereinheiten) des Gerätes freigelegt, so können die darauf befindlichen Daten ausgelesen werden (zur gleichen Ansicht kommt das Gutachten von *@stake* [2]). Das bedeutet: sollte das Gerät in fremde Hände gelangen, so ist davon auszugehen, dass die darauf befindlichen Daten kompromittiert werden können. Da aufgrund der „Push-Technologie“ von BlackBerry weiterhin Nachrichten an das Gerät gesendet werden, ist weiters davon auszugehen, dass Nachrichten, die bis zur Deaktivierung des Zugangs durch den Enterprise Server Administrator weiterhin gesendet werden, auch kompromittiert werden. Es hängt in diesem Fall vom Benutzer des BlackBerries ab, den Administrator schnellstmöglich über den Verlust in Kenntnis zu setzen, um den Zugang zu sperren (der Benutzer kann den Zugang selbst nicht sperren [3]). Das Sperren der SIM-Karte über die Mobilkom reicht als Zugangssperre nicht aus, da die Verbindungsdaten (d.h. der 3DES-Key) am Gerät verbleiben. Durch Austausch der SIM-Karte mit einer anderen für BlackBerry/Mobilkom freigeschaltenen Karte kann der Zugang wiederhergestellt werden.

Da jedes Gerät seinen eigenen Schlüssel besitzt, gibt es keine Auswirkungen auf Geräte anderer User, wenn ein Handheld in falsche Hände gelangt. Daten anderer User sind nur dann gefährdet, wenn sie sich auf dem verloren gegangenen Gerät befinden.

Werden Benutzerdaten am Gerät gelöscht, so werden die entsprechenden Bereiche im Speicher mehrmals mit Nullen und Einsen überschrieben. Diese Daten können danach nicht wieder hergestellt werden. Somit können bei Verlust des Gerätes diese Daten nicht mehr kompromittiert werden [3].

[1] BlackBerry Enterprise Server version 3.5 and version 3.6 Security White Paper for Microsoft Exchange, “BlackBerry Wireless Handheld“, Seite 5.
[2] @Stake Security Assessment http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/645094/An_@stake_Security_Assessment.pdf?nodeid=644990&vernum=0
[3] Mobilkom Österreich
[4] BlackBerry IT Policy Manager, Seite 15 „Handheld security settings“.

3. Applikationssicherheit

Für BlackBerries ab der Handheld Software Version 3.6 besteht die Möglichkeit, Java Applikationen drahtlos über den BlackBerry Browser zu installieren. Zwar unterliegen diese Applikationen denselben Einschränkungen, denen alle J2ME MIDlets [1] unterliegen, allerdings bietet das Gerät API Funktionen an, die über die Möglichkeiten der J2ME Spezifikation hinausgehen. MIDlets können nur auf den Speicher des Handhelds zugreifen, der für die JVM reserviert ist. Ein Zugriff auf andere am Handheld befindliche Daten ist für MIDlets grundsätzlich nicht vorgesehen, allerdings bieten die BlackBerry Geräte eine erweiterte API an. Diese API erlaubt unter anderem einen Zugriff auf Netzwerkressourcen, Telefonbucheinträge etc. Die erweiterte Funktionalität kann nur von MIDlets verwendet werden, die von Research In Motion (RIM) [3] digital signiert worden sind. Allerdings werden von RIM keinerlei Untersuchungen der MIDlets vorgenommen [2], es wird lediglich registriert, wer (welche Person oder Firma) diese API verwendet. Die Entscheidung, ob einer Applikation vertraut wird, liegt beim Anwender. Es erfolgt keine Zertifikatsprüfung. Ob einer Anwendung vertraut wird oder nicht kann auch nicht durch eine Policy geregelt werden.

Generell können nur Java Applikationen installiert werden – es können keine anderen Programme (C, C++ etc.) verwendet werden [4]. Die Installation von Fremdsoftware kann durch eine entsprechende Policy gänzlich unterbunden werden. Der Benutzer hat darüber hinaus keine Möglichkeit, eine bestehende Policy zu umgehen bzw. die Verwendung der Policy auszuschalten [4].

[1] Java 2 Platform, Micro Edition (J2ME), http://java.sun.com/j2me/
[2] Application Security for Java-based Handhelds
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8179/271479/Application_Security_for_Java-based_BlackBerry_Handhelds.pdf?nodeid=328385&vernum=0
Kap. “Controlled access to handheld resources”, Seite 4
[3] Controlled APIs, http://www.blackberry.com/developers/na/java/tools/controlledAPIs.shtml
[4] Mobilkom Österreich

4. Optionale Komponenten

S/MIME Support Package

Die Firma BlackBerry bietet optional ein Softwarepaket für die Versendung von S/MIME signierten/verschlüsselten Nachrichten an. Dieses Paket bietet eine end-to-end Sicherung der Daten an (d.h. wenn die Nachricht am Handheld verschlüsselt wird, wird sie erst wieder beim Empfänger entschlüsselt und nicht an einer Zwischenstation), allerdings benötigt man dafür ein entsprechendes Zertifikatsmanagement und eine PKI Infrastruktur.

Die Installation von Zertifikaten am Handheld erfolgt - sofern nicht in der Nachricht enthalten - über den Desktop PC, wenn sich das Gerät in der Cradle befindet. Zusätzlich kann über den Enterprise Server ein Zertifikatssuchdienst angeboten werden, der das entsprechende Zertifikat sucht, überprüft und über die drahtlose Verbindung an den Handheld weiterleitet. Zertifikate denen der Benutzer vertraut, kann er selbst festlegen. Verschlüsselte Attachments werden am Enterprise Server nicht konvertiert.

[1] BlackBerry S/MIME Support Package, BlackBerry Security with the S/MIME Support Package

Desktop Redirector

Anstelle eines Enterprise Servers ist es möglich, Mails über den Desktop PCs des Benutzers weiterzuleiten [1]. Dabei übernimmt eine am PC des Users installierte Software – der so genannte „Redirector“ – das Weiterleiten der Nachrichten. Ebenso wie beim Enterprise Server werden die Nachrichten vom Exchange Server geholt, verschlüsselt und weitergeleitet. Diese Art der Weiterleitung von Nachrichten ist bei einer vorhandenen Enterprise Server Installation nicht möglich [1].

[1] BlackBerry redirector Software, BlackBerry Desktop Redirector
[2] Mobilkom Austria

Zusammenfassung

Das BlackBerry Mobile Data Service wurde entwickelt, um Benutzern einen sicheren Zugriff auf ihre im Firmennetzwerk befindlichen Daten zu ermöglichen. Den Kern dieses Service bilden der BlackBerry Enterprise Server und ein Mailserver. Bei der Wahl des Mailservers ist man jedoch auf den Microsoft Exchange Server oder den Lotus Domino Server festgelegt. Bei der Wahl der Endgeräte ist man derzeit auf Handhelds der Firma BlackBerry beschränkt. PDAs und SmartPhones anderer Hersteller werden laut [1] in Zukunft auch RIM Technologie unterstützen und sich in dieses System integrieren lassen.

Die sicherheitstechnischen Eigenschaften des Blackberry können mit denen eines Notebooks verglichen werden. Die Kommunikation mit dem Intranet/Mailserver wird VPN-ähnlich abgesichert, die lokal gespeicherten Daten sind nur durch ein Passwort geschützt und liegen ungesichert im Speicher. Die größte Schwachstelle ist daher der mögliche Verlust oder Diebstahl des Gerätes, der Zugriff auf die gespeicherten Daten möglich macht. Die Schutzmaßnahme der Löschung der Daten, die vom Systemadministrator ausgelöst werden kann, kann leicht umgangen werden.

Es lässt sich durchaus eine Empfehlung für dieses System aussprechen, sofern folgenden Empfehlungen Folge geleistet wird:

- Es sollten unbedingt Geräte ab Version 4.0 verwendet werden. Neben einem vereinfachten Schlüsseltausch über die drahtlose Verbindung – die Schlüsselerzeugung am Desktop PC und die darauf folgende Synchronisation mit dem PC ist nicht mehr notwendig – bieten diese Handhelds auch eine verschlüsselte Speicherung der Daten an [1].

Außerdem sollte für einen sicheren Einsatz eine Policy definiert werden, die folgende Kriterien erfüllt:

- Dem Anwender sollte es nicht erlaubt werden, Applikationen zu installieren.
- Die Wahl der Passworte sollte entsprechend den Richtlinien von BlackBerrry erfolgen (Länge, Komplexität). Die Länge des Passwortes sollte außerdem in Abhängigkeit der möglichen Fehlversuche erfolgen z.B.: 3 Fehlversuche → mehr als 4 Zeichen langes Passwort. Je länger das Passwort ist, desto mehr Fehlversuche können erlaubt werden. Aus Gründen der Benutzbarkeit sollte hier ein vernünftiger Kompromiss zwischen Fehlversuchen und Passwortlänge gefunden werden. Die Anzahl der Fehlversuche muss auf jeden Fall begrenzt sein.
- Der Desktop Redirector sollte von Benutzern nicht verwendet werden dürfen (bei Existenz eines Enterprise Servers ist dies automatisch der Fall).
- Es sollte für jeden drahtlosen Schlüsseltausch ein neues Passwort verwendet werden.
- Der Passwortschutz für den Handheld sollte aktiviert sein.
- Der User sollte sein Passwort periodisch ändern müssen.
- Die Periode bis zur Aktivierung des Bildschirmschoners sollte nicht zu groß gewählt werden.
- Es sollte ein periodischer Schlüsselaustausch gemäß den Vorgaben von BlackBerry erfolgen.
- Die Schlüsselerstellung sollte nur am eigenen PC erfolgen (sofern dies nicht über einen Dienst erfolgt).
- Dem Benutzer muss ein Service zur Verfügung gestellt werden, um verloren gegangene Geräte sofort sperren zu lassen.

Den Benutzern der BlackBerry Handhelds müssen unter anderen folgende Umstände bewusst gemacht werden:

- Der Verlust des Gerätes muss umgehend gemeldet werden.
- Vertrauliche Dokumente sollten – wenn sie am Gerät gespeichert bleiben müssen – unbedingt verschlüsselt werden. Anderenfalls sind sie schnellstmöglich zu löschen.

- Bei Verlust des Gerätes muss mit einer Kompromittierung der Daten am Gerät gerechnet werden. Passwort und Datenverschlüsselung bieten nur einen bedingten Schutz.
- Dokumente mit hohem Vertraulichkeitsstatus sollten zusätzlich gesichert werden, um end-to-end security zu gewährleisten. Dabei sollte das S/MIME Paket zum Einsatz gelangen.
- Der Benutzer darf das Gerät nicht aus der Hand geben.
- Der Benutzer darf niemandem das Passwort verraten.
- Das Passwort sollte nicht zu kurz sein, keine leicht zu erratende Kombination sein (z.B. Name des Hundes oder des Kindes). Außerdem sollte es aus einer Mischung von Buchstaben, Zahlen und Sonderzeichen bestehen.

Um die Analyse abzurunden, wäre eine detaillierte Untersuchung der Mechanismen die für die Erzeugung der Schlüssel (insbesondere für die Erzeugung der dafür notwendigen Zufallszahlen) zu empfehlen.

[1] RIM-Deutschland

BlackBerry Sicherheitsmatrix:	
Themenbereich	
Nachrichtenübertragung im BlackBerry Sicherheitsmodell (Integrität, Vertraulichkeit, Authentifizierung)	Die Übertragung wird mittels TripleDES bzw. AES-Verschlüsselung abgesichert. Die Daten sind während der Übertragung zum Enterprise Server und zum Handheld daher für Dritte nicht lesbar. Eine Veränderung der Daten würde bei der Entschlüsselung bemerkt werden. Nur der Handheld mit dem richtigen Schlüssel hat Zugriff auf die Mailbox des entsprechenden Benutzers.
Übernehmen einer bestehenden Verbindung	Ein „hi-jacken“ einer bestehenden Verbindung ist nur mit enormem Aufwand (es muss sowohl die GSM/GPRS Verbindung als auch die verschlüsselte BlackBerry Verbindung, die ähnlich einem VPN Kanal funktioniert, übernommen werden) möglich und daher äußerst unwahrscheinlich.
Verschlüsselte Nachrichten	Nachrichten werden automatisch bei der Übertragung zum und vom Enterprise Server verschlüsselt.
Verschlüsselte Attachments	Attachments werden ebenso wie Nachrichten automatisch bei der Übertragung zum und vom Enterprise Server verschlüsselt
Sicherheit der Daten am Gerät	Das Gerät bietet zwar einen Zugangsschutz, allerdings keinen Einbruchsschutz, daher ist bei Verlust des Gerätes mit der Kompromittierung der darauf befindlichen Daten zu rechnen.
Verschlüsselte Nachrichten an Adressen außerhalb der Firma senden	Die verschlüsselte Verbindung endet beim Enterprise Server. Ob Nachrichten nun vom Exchange Server verschlüsselt weitergeleitet werden, hängt vom Exchange Server selbst ab.

Gefahr durch Fremdsoftware	Generell können nur Java Applikationen am Gerät installiert werden. Diese wiederum müssen signiert sein und ein digitales Zertifikat von RIM besitzen, um die erweiterten API Funktionen nützen zu können. Erst unter diesen Vorraussetzungen ist ein Zugriff auf sensible Daten möglich.
Installation von Software durch den Benutzer	Hängt von der Policy ab und kann damit auch zur Gänze unterbunden werden.
S/MIME verschlüsselte/signierte Nachrichten (end-to-end Security)	Nur mit optionaler Software (siehe S/MIME Support Package). Allerdings setzt ein effizienter Einsatz dieser Lösung ein sinnvolles PKI-/ Zertifikatsmanagement voraus.
Verschiedene POP Mail-accounts (z.B. für private e-Mails)	Nur mit der letzten Generation von BlackBerry Handhelds möglich, allerdings sind Verbindungen dorthin nicht über die Standard TripleDES Verbindung gesichert. Die Verschlüsselung der Daten bleibt der Mailsoftware überlassen.
Konvertierung von Attachments	Die BlackBerry Lösung bietet ein Konvertierungs-Service an, d.h. Attachments werden vor der Übertragung an den Handheld konvertiert um dort, der Leistung des Gerätes entsprechend, dargestellt werden zu können. Wird allerdings das S/MIME Support Package verwendet, so können die Dokumente nicht konvertiert werden, da sie ja bereits verschlüsselt über den Enterprise Server verschickt werden. Unterstützt werden: Worddokumente, Exceltabellen, Powerpoint Folien, PDF Dokumente, WordPerfect Dateien und HTML Seiten.