

BlackBerry Security

Das Sicherheitskonzept – Übersicht und Bewertung

Dirk Fox

Die Publikation der Ergebnisse einer internen Sicherheitsanalyse des BSI durch die WirtschaftsWoche Anfang Oktober hat für erhebliches Aufsehen gesorgt. In der unveröffentlichten Studie kommen die Autoren zu dem Schluss, dass BlackBerry „auf Grund der unsicheren Architektur für den Einsatz in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“ ist. Der Beitrag stellt das Sicherheitskonzept des BlackBerry-Dienstes vor und kommt bei seiner Bewertung zu einem anderen Ergebnis.

Einleitung

In den vergangenen beiden Jahren haben BlackBerrys in Management-Kreisen und Behörden einen beeindruckenden Siegeszug angetreten. Mehr als 3,65 Millionen Nutzer sind dem „Tamagotchi für Manager“ verfallen und lassen sich unterwegs ihre E-Mails auf ihr BlackBerry SmartPhone weiterleiten. Dieser Erfolg ruft nicht nur Neider auf den Plan – zahlreiche Anbieter, darunter Microsoft und Nokia, haben inzwischen konkurrierende Lösungen angekündigt und in Vorbereitung – sondern weckt auch Sicherheitsbedenken. Denn mit der Einrichtung des BlackBerry-Dienstes im Unternehmen oder in einer Behörde ist der Zugriff auf den zentralen E-Mail-Server verbunden – ein kritischer Punkt angesichts der oft hohen Sensibilität der von Managern elektronisch ausgetauschten Nachrichten.

dem Eingang auf dem Mailserver automatisch an ein angeschlossenes BlackBerry-SmartPhone weitergeschickt. Durch leistungsfähige Filter können die weiter zu sendenden E-Mails zudem zielgenau ausgewählt werden, um den Dienst auf wichtige Nachrichten und in der Länge der Anhänge zu beschränken.

Der Vorteil der BlackBerry-Architektur gegenüber einem über eine geschützte Verbindung – wie z. B. einem Virtual Private Network (VPN) – mit dem Unternehmensnetz verbundenen Laptop liegt vor allem in der Integration des Dienstes in das SmartPhone: Die mobile Nutzung von E-Mail erfordert nur ein geeignetes Handy. Zudem ist der Dienst vollständig in die Mobilfunkverbindung integriert, daher ist keine umständliche und gegebenenfalls Fehler anfällige Installation und Aktivierung zusätzlicher Software oder Hardware (WLAN-Zugang, UMTS-Karte o. ä.) erforderlich, wie bei einem mobil angebandenen Laptop.

Weiter werden alle mobil empfangenen und auch die gesendeten E-Mail-Nachrichten auf dem E-Mail-Server des Unternehmens abgelegt – eine Synchronisation des BlackBerry-SmartPhones mit dem Unternehmens-PC ist daher nicht erforderlich. Schließlich sorgt die Push-Eigenschaft dafür, dass Nachrichten unmittelbar das BlackBerry-SmartPhone erreichen. Der Nutzer hat damit immer einen aktuellen Überblick über seinen Nachrichteneingang, und muss ihn sich nicht erst – wie bei „Poll“-Techniken üblich – aktiv durch eine Anfrage bei seinem Mailserver verschaffen.

Um den BlackBerry-Dienst in Unternehmen oder Behörden einzurichten, wird der BlackBerry Enterprise Server verwendet. Dieser Server wird im internen Netz installiert. Er entnimmt die an ein BlackBerry-SmartPhone weiter zu leitenden Nachrichten direkt den Postfächern des E-Mail-Servers des Unternehmens, wahlweise einem Exchange- (Microsoft), Lotus Domi-

1 Der BlackBerry-Dienst

Der von der kanadischen Firma Research In Motion (RIM) angebotene BlackBerry-Dienst bietet die Möglichkeit, elektronische Nachrichten (E-Mails) eines Unternehmens- oder Behörden-Accounts auf ein geeignetes SmartPhone (Handy mit Tastatur und größerem Bildschirm) umzuleiten und mobil über den unternehmenseigenen E-Mail-Server zu versenden.¹ Das SmartPhone übernimmt dabei die Rolle eines drahtlos an die E-Mail-Infrastruktur angebandenen, mobilen E-Mail-Clients: An fast jedem Ort der Welt können so die eigenen E-Mails gelesen und beantwortet werden.

BlackBerry ist ein so genannter „Push“-Dienst, d. h. E-Mails werden gleich nach

¹ Geeignete BlackBerry-fähige Endgeräte, so genannte SmartPhones, werden inzwischen nicht mehr nur von RIM, sondern auch von führenden Handy-Herstellern angeboten.



Dirk Fox
Geschäftsführer der
Secorvo Security
Consulting GmbH
und Herausgeber der
DuD. Arbeitsschwer-
punkte: PKI, PDA-
Sicherheit, Daten-
schutzfragen.

E-Mail: dirk.fox@secorvo.de

no- (IBM) oder GroupWise-Server (Novell), und liefert dort alle mobil erstellten E-Mails zur Versendung und Archivierung ab.² Zugleich unterhält der BlackBerry Enterprise Server eine Internet-Verbindung zu einem Mobile Routing Center (MRC), das für die Weiterleitung der Nachrichten über eine Mobilfunkverbindung an das Endgerät des Benutzers sorgt.³

2 Sicherheitsarchitektur

Die von RIM entwickelte BlackBerry-Sicherheitsarchitektur [RIM_05a] umfasst zahlreiche Mechanismen, die im Folgenden dargestellt werden – gegliedert in drei wesentliche Bereiche: den Schutz der über die BlackBerry-Infrastruktur übertragenen Daten, den Schutz der im SmartPhone gespeicherten Daten und den Schutz der E-Mail-Infrastruktur im Unternehmen.

2.1 Schutz der Übertragung

Der Schutz von Nachrichten, die zwischen dem BlackBerry Enterprise Server und dem BlackBerry-SmartPhone übermittelt werden, vor unbefugter Kenntnisnahme (Vertraulichkeit), Veränderung (Integrität) und Absenderfälschung (Authentizität) erfolgt auf mehreren Ebenen (siehe Abbildung).

So werden zunächst alle Nachrichten im SmartPhone bzw. dem BlackBerry Enterprise Server symmetrisch im CBC-Mode gemäß FIPS PUB 81 verschlüsselt [NIST_80], wahlweise unter Verwendung von TripleDES (112 bit Schlüssellänge, Default-Einstellung ab Version 3.6) oder AES (256 bit Schlüssellänge, ab Version 4.0). Das Verfahren wird

² Andere Mailserver wie Sendmail oder Postfix werden vom BlackBerry Enterprise Server nicht unterstützt.

³ Sollen nur wenige Mailboxen mit dem BlackBerry-Dienst ausgestattet werden, genügt die Installation des BlackBerry Redirector auf dem Arbeitsplatzrechner. Wie der BlackBerry Enterprise Server greift der Redirector auf die Mailbox des Benutzers zu und leitet von dort eingehende Nachrichten über Internet, MRC und eine Mobilfunkverbindung an das BlackBerry-SmartPhone weiter. Sicherheitstechnisch ähnelt diese Lösung dem BlackBerry Enterprise Server. Auch der direkte Zugriff via POP auf Mailboxen ist möglich; aus Sicherheitssicht unterscheidet sich diese Lösung jedoch nicht von anderen Postfachzugängen über eine mobile Internet-Verbindung. Beide Varianten werden daher nicht weiter betrachtet.

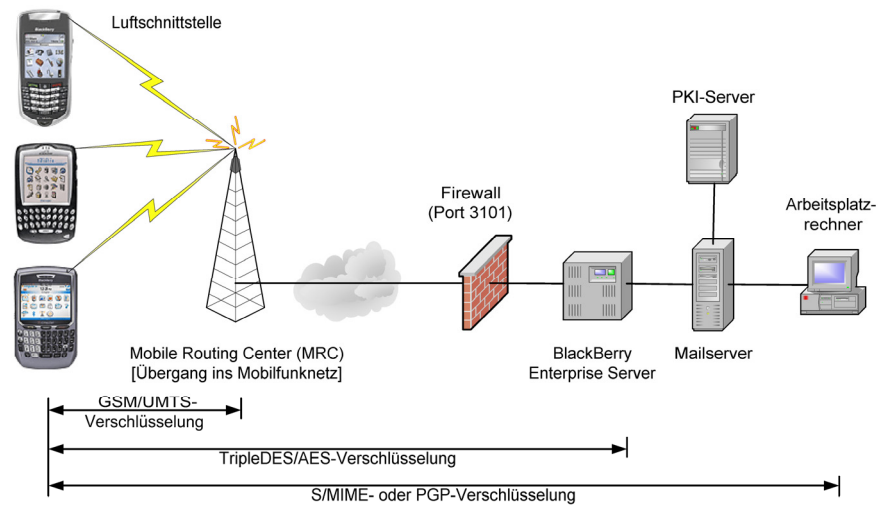


Abb.: BlackBerry-Sicherheitsarchitektur

vom Administrator gewählt.⁴ Die Integrität der verschlüsselten Daten wird nicht durch eine kryptographische Prüfsumme, sondern durch eine Kontrolle der Datenstruktur des empfangenen Pakets verifiziert – ein kryptographisch schwaches, aber praxistaugliches Verfahren, um verfälschte Pakete mit ausreichender Sicherheit identifizieren zu können.

Die Nachrichtenverschlüsselung erfolgt mit einem zufällig gewählten Nachrichtenschlüssel (message key), der verschlüsselt mitgeschickt wird. Zur Verschlüsselung des Nachrichtenschlüssels dient ein Masterschlüssel (master encryption key), der bei der Einrichtung des SmartPhones vom Benutzer auf seinem PC erzeugt und über eine direkte Synchronisation auf seinem SmartPhone sowie im persönlichen Nachrichtenverzeichnis des Nutzers auf dem Mailserver zugriffsgeschützt abgelegt wird.⁵ Dieser Masterschlüssel sollte in regelmäßigen Abständen gewechselt werden; voreingestellt ist eine monatliche automatische Neugenerierung durch die Desktop-Software. Der bei der Generierung verwendete Zufallszahlenalgorithmus wird durch Mausbewegungen des Benutzers initialisiert.

⁴ Um die Interoperabilität mit älterer oder jüngerer SmartPhone-Software aufrecht zu erhalten, können auch beide Verfahren ausgewählt werden. Dann wird ab Version 4.0 AES, bei älteren Software-Releases TripleDES verwendet.

⁵ Ab Version 4.0 kann die Schlüsselerzeugung auch durch einen zentralen Server erfolgen.

Die verschlüsselten Daten werden über das Internet an ein Mobile Routing Center (MRC) übermittelt, das für europäische Nutzer in Egham bei London steht. Dort werden die Daten an eine Mobilfunkverbindung übergeben. Die Übertragung der Nachrichten über diese „Luftschnittstelle“, d. h. die Funkstrecke des Mobilfunknetzbetreibers mit einem der gängigen Mobilfunkprotokolle GSM oder UMTS, ist durch die in den Mobilfunkprotokollen vorgesehenen Mechanismen geschützt, sofern kein Mechanismus deaktiviert ist.⁶

Die Nutzung des S/MIME bzw. des PGP Support Package (ab Version 4.0) bietet zudem die Möglichkeit, Nachrichten sensiblen Inhalts mit einem vollständigen Ende-zu-Ende-Schutz zu versehen [RIM_03, RIM_05b]: Nach der Installation einer Kopie des privaten und öffentlichen PGP- bzw. S/MIME-Schlüssels auf dem SmartPhone können Nachrichten dort entschlüsselt, verschlüsselt, digitale Signaturen erzeugt und geprüft werden. Der Zugriff auf Zertifikate und Sperrlisten (CRLs) in Verzeichnisdiensten wird vom BlackBerry Enterprise Server vorgenommen und setzt das Vorhandensein einer Public Key Infrastruktur (PKI-Server, siehe Abbildung) im Unternehmen voraus.

⁶ Bekanntermaßen kann die Verschlüsselung auf der Luftschnittstelle in GSM seitens des Netzbetreibers deaktiviert werden; von dieser Option macht beispielsweise der IMSI-Catcher gebrauch (siehe Fox, Gateway, DuD 9/1997, S. 539). Stärker sind die Sicherheitsmechanismen von UMTS (siehe Pütz/Schmitz, UMTS-Sicherheitsdienste, DuD 4/2001, S. 205 ff.).

2.2 Schutz der Daten im SmartPhone

Im SmartPhone können – neben sensiblen Daten anderer Anwendungen wie Terminen, Aufgaben, Memos oder Dokumenten – auch empfangene E-Mails gespeichert werden. Der Schutz dieser Daten hängt vom verwendeten SmartPhone ab und ist je nach Hersteller unterschiedlich realisiert.

Die von RIM angebotenen BlackBerry-SmartPhones bieten mehrere Sicherheitsfunktionen:

- ◆ Passwortschutz mit Passwörtern von vier bis 14 Zeichen Länge; schwache Passwörter werden abgewiesen.
- ◆ Fehleingabezähler, der nach max. 10 missglückten Passwordeingaben die Löschung aller Daten des Benutzers auf dem SmartPhone auslöst.
- ◆ Verschlüsselung lokal gespeicherter Daten mit AES (ab Version 4.0).
- ◆ Passwortgeschützter Bildschirmschoner, der nach einem einstellbaren Intervall einen unbefugten Zugang zum Gerät verhindert, indem Tastatur, USB- und Infrarotschnittstelle gesperrt werden.
- ◆ Möglichkeit zur Remote-Aktivierung der Löschung aller lokalen Daten nach einer Verlust- oder Diebstahlmeldung.
- ◆ Mehrfaches Überschreiben des Flash-Speichers mit Einsen und Nullen nach einer Datenlöschung.

Die Sicherheitsfunktionen (Passwordeigenschaften, Passwortnutzung, lokale Verschlüsselung) können zentral im BlackBerry Enterprise Server konfiguriert werden. Von dem gewählten Passwort wird auf dem SmartPhone nur der SHA-1-Hashwert gespeichert.

Auf BlackBerry-SmartPhones können Java-Applets übertragen und ausgeführt werden. Eine erweiterte API erlaubt neben den Funktionen der J2ME-Spezifikation den Zugriff auf lokale Daten wie die Telefonbucheinträge; deren Nutzung ist jedoch auf von RIM digital signierte MIDlets beschränkt [A-SIT_04]. In der zentralen Policy kann die Installation von zusätzlicher Software jedoch auch vollständig unterbunden werden.

2.3 Schutz des Zugriffs auf den E-Mail-Server

Geht für einen als BlackBerry-Nutzer eingetragenen Empfänger eine E-Mail auf dem Mailserver des Unternehmens ein, wird eine Text-Kopie dieser E-Mail an den Black-

Berry Enterprise Server weitergeleitet. Dieser prüft, ob die E-Mail den vom Empfänger für die Weiterleitung eingestellten Filterbedingungen entspricht; wenn ja, wird die E-Mail verschlüsselt an das BlackBerry-SmartPhone weitergesendet, anderenfalls verworfen.

Alle erforderlichen administrativen Informationen wie die Benutzernamen, die eingestellte Verschlüsselungskonfiguration und die Authentifikationsschlüssel des Mailserver werden in einem Administrator-Account auf dem Mailserver abgelegt. Nutzerspezifische Informationen wie das SmartPhone-Passwort, der Masterschlüssel und die Filterregeln werden in einem zugriffsgeschützten „Hidden Folder“ des Benutzers (Exchange) gespeichert bzw. geschützt durch Zugriffslisten (ACL) und teilweise zusätzlich verschlüsselt in der „BlackBerryProfiles.NFS“ (Domino) abgelegt.

Der Zugriff des BlackBerry Enterprise Servers auf den Mailserver einer Behörde oder eines Unternehmens ist durch dessen Authentifikationsmechanismen und die verwendeten Kommunikationsprotokolle geschützt. Wird kein Verschlüsselungsprotokoll für die Übertragung im internen Netz verwendet, erfolgen die Zugriffe im Klartext.

3 Bewertung

3.1 Schutz der Übertragung

Die von BlackBerry verwendeten Verschlüsselungsverfahren zum Schutz der Daten vor unbefugter Kenntnisnahme, TripleDES und AES, sind nach heutigem Kenntnisstand kryptographisch sicher. Auch bieten die verwendeten Schlüssellängen (112 bit für TripleDES und 256 bit für AES) ausreichenden Schutz vor Brute Force Attacken. Für den Schutz sehr sensibler Informationen sollte AES bevorzugt werden, da es auf Jahrzehnte hinaus unmöglich sein wird, selbst mit der höchstmöglichen Konzentration an Rechenleistung einen 256 bit langen Schlüssel zu kompromittieren.

Ein Brute Force Angriff auf die Nachrichtenverschlüsselung wird zudem in der Praxis durch eine vorausgehende Kompression der Nachrichten erschwert. Damit steigt der Aufwand für einen Angreifer, festzustellen, ob ein geratener Schlüssel die Daten korrekt entschlüsselt.

Weiter erhöht die Verwendung eines jeweils neu gewählten Nachrichtenschlüssels die

Sicherheit, da von einer erfolgreichen Schlüsselattacke nur eine einzige Nachricht betroffen ist. Ein Brute Force Angriff auf den Masterschlüssel, mit dem der jeweilige Nachrichtenschlüssel verschlüsselt wird, kann nur mit Kenntnis des richtigen Nachrichtenschlüssels gelingen⁷, hat also einen erfolgreichen Angriff auf einen Nachrichtenschlüssel zur Voraussetzung.

Die Güte der Verschlüsselung hängt neben der gewählten Schlüssellänge und dem Algorithmus allerdings auch von der Qualität der Implementierung ab. Diese muss den Kryptoalgorithmus fehlerfrei implementieren und insbesondere für die Wahl des Nachrichtenschlüssels einen sicheren Zufallszahlengenerator verwenden. Da die Verschlüsselung nur systemintern erfolgt, ergibt sich die Korrektheit der Implementierung nicht implizit aus der Interoperabilität mit Komponenten anderer Hersteller.

Die Korrektheit und Güte lässt sich glaubwürdig nur durch eine externe Prüfung belegen, entweder durch ein unabhängiges Gutachten oder durch eine Sicherheitszertifizierung. Für die kryptographischen Module der SmartPhone Software in den Versionen 3.8 und 4.0 sowie die Implementierung im BlackBerry Enterprise Server erhielt RIM Anfang 2005 ein entsprechendes FIPS 140-2-Zertifikat [NIST_01], Voraussetzung für die Zulassung bei amerikanischen Bundesbehörden.

Die FIPS 140-2-Zertifizierung umfasst Sicherheitsdesign, Schnittstellen, Rollen und Dienste, physische Sicherheit, Software-sicherheit, Schlüsselmanagement sowie die kryptographischen Algorithmen einschließlich des Zufallszahlengenerators. An der Korrektheit und Qualität der Implementierung und der Güte des Zufallszahlengenerators dürfte daher kein Zweifel bestehen. Zudem benötigt ein Angreifer Zugang zur Internet-Verbindung, da ein Abhören auf der Luftschnittstelle durch die Sicherheitsprotokolle von GSM bzw. UMTS zumindest erschwert wird, auch wenn der GSM-Verschlüsselungsalgorithmus A5 und die in einigen Ländern eingesetzten Varianten A5* und A5/2 als kryptographisch schwach gelten.

⁷ Ein Brute Force Angriff setzt voraus, dass der Angreifer entscheiden kann, ob nach einem Entschlüsselungsversuch die Klartextnachricht vorliegt. Da diese, nämlich der Nachrichtenschlüssel, aus einer zufällig gewählten Bitfolge besteht und somit keine Redundanz besitzt, kann ein Angreifer bei einer Brute Force Attacke den richtigen Masterschlüssel nur identifizieren, wenn er den Nachrichtenschlüssel kennt.

3.2 Schutz der Daten im SmartPhone

Wird die verschlüsselte Speicherung der Daten auf dem SmartPhone durch die zentrale Policy erzwungen und genügt die Passwortqualität üblichen Mindestanforderungen (alpha-numerische Zeichen, mindestens acht Stellen), dann sind die Daten auch bei einem Verlust des Geräts hinreichend vor unberechtigter Kenntnisnahme geschützt. Eine von @stake durchgeführte Sicherheitsuntersuchung bescheinigt RIM eine hohe Qualität des Hardware-Designs; in der Software konnten keine typischen Fehler wie Buffer Overflows gefunden werden [stake_03]. Für mehrere BlackBerry-SmartPhones liegen zudem aktuelle FIPS 140-2-Zertifizierungen vor. In sensiblen Bereichen sollte jedoch die Installation von Java-Applets auf dem SmartPhone zentral unterbunden werden.

3.3 Schutz des Zugriffs auf den E-Mail-Server

Alle für einen auf der BlackBerry-Userlist vermerkten Empfänger eingehenden E-Mails werden vom Mailserver an den BlackBerry Enterprise Server in Kopie weitergeleitet (Exchange) bzw. durch regelmäßiges Abfragen des Mailaccounts (Domino) ausgelesen. Zwar werden nur die Nachrichten an das mobile SmartPhone weitergeleitet, die den vom Benutzer konfigurierten Filterregeln entsprechen; der BlackBerry-Server erhält zunächst jedoch Zugriff auf alle Nachrichten. Der korrekten Implementierung auf dem BlackBerry Enterprise Server muss man daher vertrauen.

Da der Server nicht von außen erreicht werden muss, sondern die verschlüsselte Übermittlung von Nachrichten über TCP/IP (Port 3101) an ein MRC und von dort weiter an ein SmartPhone vom Enterprise Server initiiert wird, ist es nicht erforderlich (und aus Sicherheitsgründen nicht zu empfehlen), den Server in einer DMZ zu betreiben. Um den Server vor Angriffen aus dem internen Netz zu schützen, sollte der BlackBerry Enterprise Server zudem auf einem gehärteten System installiert werden.

Fazit

Die BlackBerry-Sicherheitsarchitektur genügt höchsten Anforderungen und entspricht sowohl konzeptionell als auch in der Implementierung – das belegen die unabhängigen Gutachten und die FIPS 140-2-Zertifizierung – dem Stand der Technik.

Sofern durch eine strenge zentrale Konfiguration die auf den SmartPhones gespeicherten Daten durch Verschlüsselung und gute Passwörter vor unberechtigtem Zugriff bei Verlust geschützt sind, kann ein Dritter nur mit Kenntnis der Verschlüsselungsschlüssel auf die übertragenen Nachrichten zugreifen, denn die verwendeten Algorithmen und Schlüssellängen schützen auch vor einer Brute Force Attacke eines mit erheblicher Rechenleistung ausgestatteten Geheimdienstes.

Da außer dem berechtigten Empfänger nur der BlackBerry Enterprise Server Zugang zu den Verschlüsselungsschlüsseln hat, bleibt als einzige denkbare Sicherheitslücke nur ein Angriff durch Kompromittierung der BlackBerry-Software oder eine Hintertür, über die E-Mail-Nachrichten oder Verschlüsselungsschlüssel an Unberechtigte verschickt werden. Diesbezüglich muss derzeit dem Hersteller RIM vertraut wer-

den, da der Programmcode nicht offengelegt ist und auch kein unabhängiges Gutachten dazu existiert. Allerdings muss in gleicher Weise auch dem Hersteller des Mail-servers (IBM, Microsoft oder Novell) vertraut werden.

Und selbst dieser Bedrohung kann durch die Verwendung des S/MIME bzw. PGP Support Package begegnet werden, denn damit lassen sich sensible Nachrichten vom Sender zum Empfänger durchgängig verschlüsseln und durch eine digitale Signatur vor Fälschung schützen – mit Schlüsseln, die auch der BlackBerry Enterprise Server nicht kennt.

Literatur

- [stake_03] Eng, Chris; Levine, Matthew; Whitehouse, Ollie: *BlackBerry by Research in Motion: An @stake Security Assessment*. Research Report, November 2003.
- [A-SIT_04] Dietrich, Kurt: *Sicherheitsanalyse – BlackBerry Mobile Data Service*. Zentrum für sichere Informationstechnologie Austria, A-SIT, Version 1.0, Oktober 2004.
- [NIST_80] FIPS PUB 81: *DES Modes of Operation*, Federal Information Processing Standards Publication 81, 02.12.1980 (Change Notice 2: 31.05.1996).
- [NIST_01] FIPS PUB 140-2: *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-2, 25.05.2001 (Change Notice 2: 03.12.2002).
- [RIM_03] Research In Motion: *BlackBerry Security with the S/MIME Support Package*. Version 1.5, 2003.
- [RIM_05a] Research In Motion: *BlackBerry Security*. Release 4.0, White Paper, 2005.
- [RIM_05b] Research In Motion: *PGP Support Package*. Release 4.1, White Paper, 2005.