

Email-Push ... wer stößt hier wen

Teil 1 Das BlackBerry-Konzept von RIM

I. Allgemeines

Ursprünglich beschreibt das englische Wort blackberry eine sehr schmackhafte schwarzblaue Beerenfrucht und zwar die Brombeere. Ich kann nur sagen die schmeckt wirklich lecker! ;) Der Name BlackBerry steht jedoch seit 1999 in Kanada und den USA sowie später in Europa und seit kurzem auch in Deutschland, auf dem PDA-Markt als Begriff für eine bestimmte Art von PDA's die sich selbst, ohne eine durch den Benutzer ausgelöste Synchronisation, aktualisieren.



Bild1: Der erste BlackBerry von RIM (Modell 850)

Es sind die Geräte des kanadischen Herstellers RIM (Research in Motion) die einen besonderen E-maildienst automatisch mit sich bringen. Außerdem hatten diese Geräte, in Anlehnung an die Farbe der Brombeere, auch eine typische schwarzblaue bis dunkelviolette Farbe gehabt. Aktuell gibt es sie jedoch bereits in vielen verschiedenen Farben. Die BlackBerry's zeichneten sich vor allem durch ihre Fähigkeit zum mobilen Empfang und Senden von Emails aus. Während ältere Geräte nur mit einem speziellen Pager-Netzwerk kommunizieren konnten, sind die neuesten Geräte durchaus dazu in der Lage dies über GSM (Global System for Mobile Communications) oder CDMA (Code Division Multiple Access) via General Packet Radio Service (GPRS) durchzuführen. Was die BlackBerry's von Anfang an weiterhin auszeichnete war eine für die schnelle Texteingabe mittels des/der Daumen optimierte vollständige (QWERTY/Z-)Minitastatur unterhalb des Displays. Neue Geräte enthalten eine Telefoniefunktion was auch die Nutzung als „normales“ Telefon, besser gesagt als Smartphone, ermöglicht.



Bild 2: BlackBerry 6230 (mit Telefonfunktion)

Interessant sind die BlackBerry's nicht (nur) wegen ihres von Anfang an etwas extravaganten Aussehens geworden. Nein sie unterscheiden sich von normalen Smartphones mit Emailfunktion durch eine fast direkte Zustellung aller auf dem Mailserver eingehenden Emails an den BlackBerry, das heißt das Endgerät. Dies ist besonders für Geschäftskunden eine wichtige Funktion, da im Zuge der Kundenbindung und Terminabsprache eine zeitnahe Antwort äußerst wichtig sein kann. Durch den Mobilien Datenservice (MDS) ist es möglich auch andere Daten aus dem Firmennetzwerk - z.B. aus ERP-Systemen, Datenbanken etc. - auf dem BlackBerry zugänglich zu machen.

Alle BlackBerry's arbeiten mit einem proprietären Betriebssystem von RIM, das allerdings auch WAP und Java(J2ME) unterstützt.

II. Das BlackBerry-Konzept

Um die bisherige volumenintensive Kommunikation eines Mobilgerätes mit dem Firmenintranet und –emailserver mittels SSL (Secure Socket Layer) oder VPN (Virtual Private Network) zu umgehen, entwickelte die Firma RIM eine Erweiterung des TCP/IP (Transmission Control Protocol/Internet Protocol)-Headers die es erlaubt Datenpakete zu versenden, ohne dass sich beide Seiten, also Sender und Empfänger, kennen müssen. Jedes einzelne Datenpaket enthält eine eigene Kennzeichnung um sich beim Empfänger zu authentifizieren (auszuweisen) und damit eine sichere Datenübertragung zu gewährleisten. Umgesetzt hat dies RIM über ein dreistufiges Konzept:

- BlackBerry Enterprise Server (**BES**)
- Network Operation Center von RIM (**NOC**)
- mobiles Endgerät (**BlackBerry**[-Client])

1) **BES**

Der BES selbst ist ein firmeninterner Server, meist hinter einer Firewall, der Zugriff auf den firmeninternen Email-Server hat. Im Firmenalltag bedeutet dies aber nicht nur die einfache Zustellung von eingegangenen Emails, sondern auch die Aktualisierung von Kontakten und Terminen. Je nach unterstütztem Service (Exchange, Domino/Notes, Groupwise) lässt er sich benachrichtigen oder fragt selbst in kurzen Perioden die Postfächer aktiv ab. Sobald eine neue Aktivität (Termin, Kontakt, Email) vom **BES** erkannt wurde schickt er die daran hängenden Daten in 2 Kilobyte-Häppchen an das NOC. Anhängende PDF-Dateien oder Bilder werden dafür in ein eigenes Format komprimiert. Dabei kommuniziert der **BES** über ein von RIM entwickeltes Server Routing Protocol (SRP) über eine TCP/IP-Verbindung.

2) **NOC**

Die **NOC** stellen nun die „Router“ dar, über die der dynamisch verschlüsselte Datenaustausch ausgeführt wird. Eines der 3 von RIM eingerichteten überregionalen **NOC** nimmt dann die Pakete des **BES** an und leitet sie an den für das (gewünschte) Mobilfunknetz zuständigen Provider weiter. Der Vergleich des **NOC** mit einem Router ist auch insoweit gut gewählt, da die **NOC** lediglich die an sie gesendeten Datenpakete weiterleiten ohne sie zu speichern. Das einzigste was die **NOC** speichern ist eine Liste der in ihrem „Einzugsbereich“ vorhandenen und angemeldeten Endgeräte.

Übrigens befindet sich das für Europa zuständige **NOC** in Großbritannien.

3) Das Endgerät –der **BlackBerry** [-Client]

Der BlackBerry[-Client] (als Endgerät) im Mobilfunknetz ist durch seine IP-Adresse bekannt, die er automatisch erhalten hat, nachdem er sich im Mobilfunknetz angemeldet hatte. Nach der Anmeldung sendet der BlackBerry dann seine IP-Adresse mit Kommunikations-ID und seiner BlackBerry-PIN an das **NOC**, wo diese dann hinterlegt wird. Ab diesem Zeitpunkt ist der BlackBerry durch das **NOC** erreichbar.

Die gesamte Kommunikation zwischen **BES**, **NOC** und **BlackBerry** erfolgt nach dem Triple Data Encryption Standard (3DES) oder Advanced Encryption Standard (AES) ohne Masterkey von RIM. Neben der über symmetrische Privatschlüssel abgesicherten Verbindung beherrscht der BES ab Version 3.6 auch Secure/Multipurpose Internet Mail Extension (S/MIME).

Ab der Version 4.0 des **BES** wird von RIM auch eine Unterstützung für Anbieter von Drittsoftware auf dem BlackBerry ermöglicht, die erstmals gezielte Zugriffe der Endgeräte auf nur bestimmte (firmenrelevante) Daten möglich macht. Mit der zum Jahresanfang 2006

Der Artikel ist erschienen in Ausgabe 37 (November 2005) von PalmPaper... dem etwas anderen PDA-Magazin (erreichbar unter: <http://www.palmpaper.de/palmpaper.php>)

verfügbaren Version 4.1 wurde dann sogar die gezielte Versorgung der Endgeräte mit der jeweils zutreffenden Drittanbietersoftware sowie Ihre eventuelle Sperrung möglich.

4) Privatanwender

Damit auch Privatanwender den vollen Funktionsumfang des BlackBerry nutzen können, stellen die Mobilfunkprovider Server, analog den **BES**, zur Verfügung, die den Basisdienst Email bereitstellen. Bereits vorhandene Emailpostfächer bei anderen Providern müssen dann auf das Emailpostfach (den Quasi-BlackBerry-Server) des Mobilfunkproviders weitergeleitet werden.

III. Weitere Informationen

1) Sicherheitsaspekt

In den letzten Wochen erschienen einige Informationen zur mangelhaften Sicherheit bei der BlackBerry-Architektur. Diese wurden zum einen geäußert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und zum anderen von der Seite potentieller Kunden wie zum Beispiel der Volkswagen AG (insbesondere Audi). Der eigentlich nur für den internen Gebrauch bestimmte Bericht des BSI kennzeichnet die Architektur als „in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“. Der Hauptkritikpunkt ist dabei das in Egham bei London (Großbritannien) befindliche **NOC**, das dem britischen Recht unterworfen ist. Hier wird der durch den RIP Act (Regulation of Investigatory Powers Act 2000) zur Terrorismusbekämpfung autorisierte Zugriff britischer Sicherheitsbehörden, die bekanntlich sehr eng mit der NSA (National Security Agency) der USA bei dem Echelon genannten Abhörprojekt gegen andere Wirtschaftsnationen zusammen arbeiten, befürchtet. Diese Argumentation konnte RIM bisher „nicht nachvollziehen“. Durch das Fehlen eines Masterkey's bestehe kein direkter Zugriff auf die in den **NOC** durchgeschleusten Datenpakete und damit werden die durch das BSI erhobenen Sicherheitsmängel lediglich als theoretischen Abhörmöglichkeiten angesehen.

Um diese Vorwürfe über Sicherheitsmängel zu entkräften wurde das Fraunhofer Institut für sichere Informationstechnologie (SIT) durch RIM mit einer Sicherheits-Analyse der BlackBerry-Lösung beauftragt, um die in der BlackBerry-Architektur steckende Verschlüsselung zu prüfen. Das Ergebnis der Studie kann RIM dann interessierten Kunden zur Verfügung stellen. Als Ergebnis wird dann eine allgemeingültige Sicherheitsbewertung für die drahtlose Kommunikationsplattform BlackBerry erwartet.

Von Utimaco wurde jetzt zur Beruhigung eventuell verunsicherter (potentieller) Kunden eine SafeGuard PushMail genannte Sicherheitlösung entwickelt und für Blackberry angeboten. Dabei werden alle Mails mit OpenPGP oder S/MIME bereits auf dem Server verschlüsselt und dann auf den Blackberry-PDA übertragen.

2) unterstützte Plattformen

BlackBerry-Client-Anwendungen, die in der oben beschriebenen Architektur von RIM arbeiten (können) sind aktuell nicht nur für BlackBerry-Geräte verfügbar. Zwischenzeitlich wurden diese auch für WindowsCE/WindowsMobile und SymbianOS/UIQ entwickelt.

Vor kurzem wurde die BlackBerry-Lösung auch für PalmOS Garnet veröffentlicht.

Der BlackBerry-Client ist ab sofort für den Palm Treo 650 verfügbar, der sich dann „BlackBerry® Connect™ to the Palm® Treo™ 650 smartphone“ nennt. Der entsprechende Client wird aktuell jedoch zur Einführung nur auf dem asiatischen Kontinent angeboten (siehe [Link unten](#)).

3) Internetadressen

Firma RIM: <http://www.rim.com/>

Downloadlink zum BlackBerryConnect-Client für den Treo 650:

<http://www.palm.com/sg/solutions/products/blackberryconnect/getitnow.html>

Updatet 20.04.06