

ERNW Newsletter 27 / Juni 2009

Liebe Partner, liebe Kollegen,

willkommen zur 27. Ausgabe des ERNW-Newsletters mit dem Thema:

Untersuchung zur Sicherheit der Over-the-air- Erzeugung von Master Encryption Keys zwischen BlackBerry-Geräten und dem BlackBerry Enterprise Server

Version 1.0 vom 7. Juni 2009

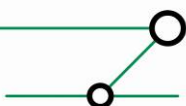
von: Friedwart Kuhn (fkuhn@ernw.de)

Abstract

Dieses Dokument analysiert und bewertet die Sicherheit der Erzeugung von Master Encryption Keys zur Inbetriebnahme von BlackBerry-Geräten und für das automatische Update von Master Encryption Keys zwischen BlackBerry-Geräten und dem BlackBerry Enterprise Server. Die technische Analyse wird von flankierenden Maßnahmen-Empfehlungen zum sicheren Einsatz begleitet.



1	EINLEITUNG	3
2	UNTERSUCHUNG ZUR SICHERHEIT DER OVER-THE-AIR-ERZEUGUNG DES MASTER ENCRYPTION KEY BEI DER INBETRIEBNAHME VON BLACKBERRY-GERÄTEN UND BEIM SCHLÜSSEL-UPDATE MIT DEM BLACKBERRY ENTERPRISE SERVER	4
2.1	Voraussetzung und Abgrenzung	4
2.2	Untersuchte Software-Version.....	4
2.3	Funktionsweise der Over-the-Air-Erzeugung des Master Encryption Key	4
2.3.1	Grundsätzliches	4
2.3.2	Zum Einsatz gelangende Schlüssel	5
2.3.3	OTA-Erzeugung des Master Encryption Key bei der Wireless-Inbetriebnahme	6
2.3.4	OTA-Erzeugung eines Master Encryption Key beim Master Encryption Key-Update	7
2.4	Mögliche Bedrohungen und Schwachstellen bei der Over-the-air-Masterkey-Erzeugung	7
2.4.1	Mögliche technische Bedrohungen und Schwachstellen	7
2.4.2	Mögliche organisatorische Bedrohungen und Schwachstellen.....	8
2.5	Bewertung der Bedrohungen und Schwachstellen	8
2.5.1	Impersonierung des Servers aus der Sicht des Clients durch einen Angreifer gemäß [Tang, 2005]	8
2.5.2	Session-Instanziierung während der Erzeugung des geheimen Schlüssels gemäß [Tang, 2005]	9
2.5.3	Auswirkung möglicher unzureichender Realisierung von idealen Zahlenmodellen in ‚Geschwisterprotokollen‘ gemäß [Zhao, 2005]	9
2.6	Bereits implementierte Schutzmaßnahmen	10
2.7	Zusätzlich empfohlene Schutzmaßnahmen	10
2.8	Fazit	11
3	QUELLEN	12



1 EINLEITUNG

BlackBerry-Sicherheit ist ein Thema, das seit dem Erscheinen der BlackBerrys immer wieder für Furore und ‚heiße Diskussionen‘ gesorgt und die Sicherheit der Geräte sowie der dazugehörigen Infrastruktur infrage gestellt und auf den Prüfstand gebracht hat. Zuletzt in der aktuellen und bisher wohl umfassendsten Untersuchung durch das Fraunhofer SIT, die alle beteiligten Komponenten der BlackBerry Enterprise-Lösung einer differenzierten Sicherheitsanalyse, die sowohl technische wie organisatorische Aspekte berücksichtigt, unterzogen hat¹. Gleichwohl untersucht dieses Studie nicht das für den großflächigen Rollout relevante Szenario der „Wireless“- oder „Over-The-Air“-Inbetriebnahme von BlackBerry-Geräten sowie das für den Enterprise-Betrieb interessante Szenario der „Wireless“- oder „Over-The-Air“-Erneuerung von Verschlüsselungsschlüsseln. Damit können BlackBerry-Geräte ohne physische Verbindung zu einem LAN oder zu einem Arbeitsplatz-PC (auf dem dann die BlackBerry-Desktop Software installiert sein muss) in Betrieb genommen und (dauerhaft) betrieben werden. Die Aushandlung des wichtigen Master Encryption Keys erfolgt dabei (sowohl initial als auch dann im dauerhaften Betrieb) über das ‚Shared-Medium‘ Luft. Da dieser Prozess ausgesprochen sicherheitssensitiv ist und es bisher keine dedizierte Analyse dieses Prozesses gibt, schließt die nachfolgende Untersuchung diese Lücke.

¹ Siehe [Fraunhofer BBSec, 2008].



2 UNTERSUCHUNG ZUR SICHERHEIT DER OVER-THE-AIR-ERZEUGUNG DES MASTER ENCRYPTION KEY BEI DER INBETRIEBNAHME VON BLACKBERRY-GERÄTEN UND BEIM SCHLÜSSEL-UPDATE MIT DEM BLACKBERRY ENTERPRISE SERVER

2.1 Voraussetzung und Abgrenzung

Die vorliegende Untersuchung ist mit Analyse und Bewertung auf die Sicherheit des Prozesses der Over-The-Air-Erzeugung von Master Encryption Keys konzentriert. Angrenzende Sicherheitsaspekte wie Betriebssystem- oder Mailservericherheit stehen nicht im Fokus dieser Untersuchung. Insbesondere wird vorausgesetzt, dass die dem BlackBerry Enterprise Server zugrunde liegende Betriebssystem- und Mailserverkonfiguration auf der Höhe aktueller Sicherheitsstandards und Best Practices erfolgt. Dies wird deshalb explizit erwähnt, weil die Over-The-Air-Erzeugung von Master Encryption Keys erfordert, dass der Master Encryption Key in der Mailbox-Verzeichnisstruktur des Benutzers gespeichert wird.

2.2 Untersuchte Software-Version

Die in diesem Dokument durchgeführte Untersuchung bezieht sich auf die Black Enterprise Server-Software ab der Version 4.1 SP5 zusammen mit BlackBerry-Endgeräten mit einer Firmware ab der Version 4.5.

2.3 Funktionsweise der Over-the-Air-Erzeugung des Master Encryption Key

2.3.1 Grundsätzliches

Der für die verschlüsselte Kommunikation zwischen einem BlackBerry-Gerät und dem BlackBerry Enterprise Server (dem sog. BES) verwendete Master Encryption Key wird abhängig von der Art, wie das Gerät mit seiner Umgebung verbunden ist, auf zwei unterschiedliche Weisen erzeugt. Wenn das BlackBerry-Gerät mit dem Desktop des BlackBerry-Benutzers verbunden ist, wird der Master Encryption Key von der BlackBerry Desktop Software auf dem Computer des Benutzers erzeugt und von ihr sowohl an das angeschlossene BlackBerry-Gerät als auch (via LAN) an den BES gesendet. Wenn sich das BlackBerry-Gerät in der Wireless-Umgebung der Organisation befindet (und nicht über das Kabel mit dem Desktop des BlackBerry-Benutzers verbunden ist), wird der Master Encryption Key unter Aushandlung der zu verwendenden Algorithmen mit dem BES „Over-The-Air“ (üblicherweise und auch in diesem Dokument durch OTA abgekürzt) auf dem BlackBerry-Gerät und dem BES erzeugt (genaue Beschreibung weiter unten).² Die in diesem Dokument durchgeführte Untersuchung beschränkt sich auf die Sicherheitsuntersuchung der Over-the-Air-Erzeugung des Master Encryption Keys.

Die OTA-Erzeugung von Master Encryption Keys umfasst ihrerseits zwei unterschiedliche Szenarien:

- die OTA-Erzeugung des Master Encryption Keys bei der (erstmaligen) Inbetriebnahme des BlackBerry-Geräts in Wireless-Umgebungen
- die OTA-Erzeugung des Master Encryption Keys beim (regelmäßigen) Update des Master Encryption Keys in Wireless-Umgebungen

Die beiden Verfahren unterscheiden sich dabei in den für die Schlüsselerzeugung verwendeten Protokollen (siehe dazu die Abschnitte 4.2.3f).

² Die Over-the-air-Erzeugung des Master Encryption Key ist erst mit der BlackBerry-Software ab Version 4.0 möglich. Bis dahin war die Erzeugung des Master Encryption Key nur mittels der BlackBerry Desktop Software möglich.



2.3.2 Zum Einsatz gelangende Schlüssel

Bei der OTA-Erzeugung des Master Encryption Keys kommen folgende Schlüssel zum Einsatz:

- ❑ **Ephemeral Key** des BlackBerry-Geräts: Dieser (symmetrische) Schlüssel wird von dem Zugangspasswort des BlackBerry-Geräts abgeleitet; es handelt sich um einen 256-bit AES-Schlüssel. Dieser Schlüssel verschlüsselt den gerätespezifischen Private Key (sowie den *Content Protection Key* unter der Voraussetzung, dass auf dem BES die Inhaltsverschlüsselung – die sog. *Content Protection* – für das Gerät aktiviert wurde³) und befindet sich auf dem BlackBerry-Gerät.
- ❑ **Private- & Public-Key-Paar des BlackBerry-Geräts**: Dieses (asymmetrische) Schlüsselpaar wird während der Initialisierung des BlackBerry-Gerätes erstellt und ist einmalig für dieses Gerät. Es werden 521-bit ECC⁴-Schlüssel erstellt. Beide Schlüssel werden für die Erzeugung des Master Encryption Key benötigt und werden auf dem BlackBerry-Gerät gespeichert.
- ❑ **Private- & Public-Key-Paar des BES**: Dieses (asymmetrische) Schlüsselpaar wird während der Initialisierung des BES erstellt und ist einmalig für diesen BES. Es werden 521-bit ECC-Schlüssel erstellt. Beide Schlüssel werden für die Erzeugung des Master Encryption Key benötigt und werden auf dem BES gespeichert.
- ❑ **Master Encryption Key**: Dieser (symmetrische) Schlüssel ist der für die sichere Datenübertragung zwischen dem BES und dem BlackBerry-Gerät wichtigste Schlüssel. Er ist eindeutig für jedes BlackBerry-Gerät und wird sowohl auf dem BlackBerry-Gerät als auch dem BES gespeichert⁵. Der Master Encryption Key wird bei der OTA-Erzeugung – wie unten detailliert beschrieben – sowohl von dem BlackBerry-Gerät als auch dem BES erstellt. Es handelt sich dabei je nach Konfiguration der entsprechenden Richtlinie (Policy) auf dem BES um einen 112-bit Triple DES- oder um einen 256-bit AES-Schlüssel.

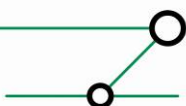
Die folgende Abbildung (nächste Seite) gibt eine Übersicht über die auf einem BlackBerry-Gerät verwendbaren⁶ Schlüssel mit ihren Interdependenzen. Bei der OTA-Erzeugung des Master Encryption Keys kommen gleichwohl nur die in diesem Abschnitt beschriebenen Schlüssel zum Einsatz.

³ *Content Protection auf BlackBerry-Geräten ist für die OTA-Erzeugung des Master Encryption Keys bedeutungslos. Gleichwohl liefert sie einen wertvollen Schutz von auf dem Gerät gespeicherten Daten, wenn das Gerät gesperrt ist (siehe auch Abschnitt 4.6).*

⁴ *ECC steht für Elliptic Curve Cryptography, ein sicheres und performantes Verfahren zur Schlüsselerzeugung in der asymmetrischen Kryptographie.*

⁵ *Darüber hinaus wird der Master Encryption Key bei der Verwendung von Microsoft Exchange oder IBM Lotus Domino als Messaging-Server-Plattform auch noch von diesen Produkten gespeichert. Dies wird nur um der Vollständigkeit Willen erwähnt, besitzt für die hier durchgeführte Untersuchung jedoch keine weitere Bedeutung (vgl. dazu auch [BB-STO], S. 9).*

⁶ *Der Content Protection Key und der Grand Master Key kommen erst dann zum Einsatz, wenn auf dem BES die dafür notwendigen Policies gesetzt sind (vgl. dazu auch [BB-PRG]).*



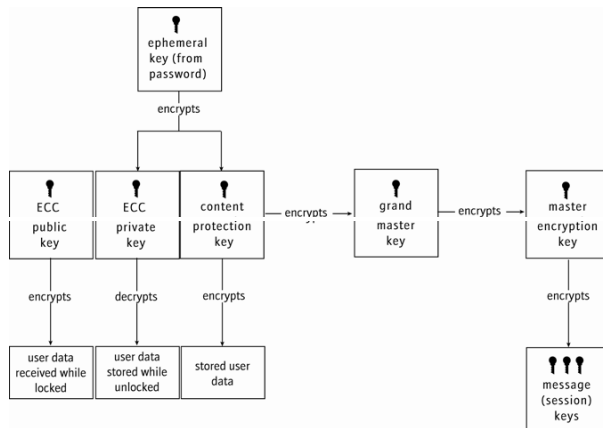


Abbildung 1⁷: Von einem BlackBerry-Gerät verwendbare Schlüssel

2.3.3 OTA-Erzeugung des Master Encryption Key bei der Wireless-Inbetriebnahme

Die OTA-Erzeugung des Master Encryption Keys bei der Inbetriebnahme des BlackBerry-Geräts in Wireless-Umgebungen wird von RIM als *BlackBerry Wireless Enterprise Activation* bezeichnet. Diese verwendet ein von RIM als *BlackBerry Initial Key Establishment Protocol* bezeichnetes Verfahren. Dieses Verfahren verwendet wiederum das in ISO 11770-4⁸ standardisierte und in IEE P1363.2⁹ spezifizierte SPEKE¹⁰-Protokoll.

Die OTA-Erzeugung des Master Encryption Key verläuft in den folgenden Schritten:

1. Der Benutzer erhält sein (noch nicht in Betrieb genommenes) BlackBerry-Gerät und dazu ein Out-of-the-Band (z. B. per Post oder Telefon) von der BES-Administration vergebene Wireless Enterprise-Aktivierungspasswort¹¹.
2. Der Benutzer initiiert die Wireless Enterprise Activation, indem er das Enterprise Activation-Programm auf dem BlackBerry-Gerät öffnet und seine E-Mail-Adresse zusammen mit seinem Aktivierungspasswort eingibt.
3. Das BlackBerry-Gerät sendet einen Aktivierungs-Request als E-Mail an die vorher eingegebene E-Mail-Adresse. Die E-Mail enthält neben dem Request Routing- und gerätespezifische Informationen sowie den öffentlichen Schlüssel des BlackBerry-Geräts.
4. Der BES antwortet auf den Request mit seinen Routinginformationen und seinem öffentlichen Schlüssel.
5. BlackBerry-Gerät und BES erzeugen aufgrund der ausgetauschten Informationen, dem geteilten (aber nicht direkt übertragenen) Aktivierungspasswort und weiterer Parameter (in die u. a. eine Transaktions-ID und sowohl der eigene private wie auch der öffentliche Schlüssel des Kommunikationspartners einfließen) den Master Encryption Key. Der Master Encryption wird über eine 256-bit HMAC-Funktion authentifiziert gehaht, und dieser Wert wird an den Kommunikationspartner übertragen und von diesem verifiziert. Wenn die Verifikation des HMAC-Wertes von jedem der beiden Kommunikationspartner erfolgreich durchgeführt wurde, wird der Aktivierungsprozess abgeschlossen, und jede weitere

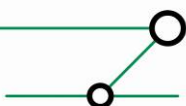
⁷ Die Abbildung ist dem Dokument [BB-STO], S. 9 entnommen.

⁸ Vgl. [ISO11770-4], Abschnitt 6.1.

⁹ Vgl. [IEEEP1363.2].

¹⁰ SPEKE steht dabei für Simple Password-authenticated Exponential Key Exchange.

¹¹ Beachte dazu auch Abschnitt 4.3.2 und 4.6.



Kommunikation zwischen BlackBerry-Gerät und BES findet ab diesem Zeitpunkt verschlüsselt¹² statt.¹³

2.3.4 OTA-Erzeugung eines Master Encryption Key beim Master Encryption Key-Update

Das von RIM als *Key Rollover Protocol* bezeichnete Verfahren sorgt dafür, dass ein in Verwendung befindlicher Master Encryption Key nicht beliebig lange verwendet werden darf, sondern spätestens nach 30 Tagen durch einen neuen Master Encryption Key ersetzt wird. Dies betrifft sowohl den über das *Initial Key Establishment Protocol* erzeugte Master Encryption Key als auch jeden weiteren erzeugten Master Encryption Key. Zum Einsatz kommt dabei das Menezes-Qu-Vanstone (MQV)-Protokoll, ein vom NIST in [SP800-56A] empfohlenes Verfahren zur paarweisen Erzeugung von Schlüsseln, das sich der asymmetrischen Kryptographie bedient. Die diese Funktion verwendenden Kryptomodule im BES und im BlackBerry-Gerät sind FIPS 140-2 zertifiziert.¹⁴

Ein neuer Master Encryption Key kann sowohl durch manuelle Initiierung auf dem BES als auch auf dem BlackBerry-Gerät erzeugt werden. Spätestens nach 30 Tagen veranlasst die BlackBerry Enterprise Software eine Neuerzeugung des Master Encryption Key zwischen BlackBerry-Gerät und BES.

2.4 Mögliche Bedrohungen und Schwachstellen bei der Over-the-air-Masterkey-Erzeugung

Es sind bisher zahlreiche Untersuchungen zu verschiedenen Sicherheitsaspekten von sowohl BlackBerry-Geräten als auch der gesamten BlackBerry-Infrastruktur vorgenommen wurden. Als exemplarisch können die in Abschnitt 3 gelisteten Studien – hier in chronologischer Reihenfolge aufgeführt – von @stake für RIM [@stake, 2003], von A-SIT für das Österreichische Bundeskanzleramt [A-SIT, 2004], von Secorvo [Secorvo, 2005], von ERNW [ERNW, 2006] und von Fraunhofer SIT für RIM Ltd. gelten. Keine dieser Studien konnte oder wollte¹⁵ sich mit der Sicherheit der OTA-Erzeugung des Master Encryption Key beschäftigen.

2.4.1 Mögliche technische Bedrohungen und Schwachstellen

Es konnten bisher nur zwei theoretische Angriffe gegen das *Initial Key Establishment Protocol* gefunden werden, die auf Schwächen im SPEKE-Protokoll zurückgehen. Diese sind:

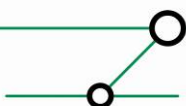
1. **Impersonierung des Servers aus der Sicht des Clients durch einen Angreifer:** Tang [Tang, 2005] beschreibt eine Lücke in der Version des SPEKE-Protokolls, die als Draft für IEEE P1363.2 vorliegt und auf die sich auch RIM in [BB-WEA] als Grundlage beruft. Die erfolgreiche Ausnutzung der Lücke führt für den Angreifer zum Besitz des geheimen Schlüssels, ohne dass die berechtigten Kommunikationsteilnehmer etwas davon erfahren. Voraussetzungen für das erfolgreiche Ausnutzen dieser Lücke sind:
 - a. Das zwischen Client und Server geteilte Geheimnis wird zwischen mehr als nur zwei Kommunikationsteilnehmern geteilt (z. B. einem zweiten Server).

¹² Unter Verwendung von Master Encryption Key und den Message Keys.

¹³ Die detailliertere mathematische Beschreibung der Erzeugung des Master Encryption Keys findet sich in [BB-WEA] S., 10ff.

¹⁴ Siehe <http://na.blackberry.com/eng/atagance/security/certifications.jsp>.

¹⁵ *Wireless Enterprise Activation setzt BlackBerry Enterprise Software v.4.0 voraus. Die Mehrzahl der aufgeführten Studien datiert vor dieser Version. Die Fraunhofer SIT-Analyse empfiehlt das Deaktivieren der Speicherung des Master Encryption Keys eines Benutzers in dessen Mailbox-Verzeichnis. Wenn dies durchgeführt wird, sind weder eine Wireless-Inbetriebnahme noch ein Wireless Master Encryption Key-Update möglich. Die vom Fraunhofer SIT zertifizierte BlackBerry Enterprise-Konfiguration verlangt die Deaktivierung aus Compliance-Gründen zur Fraunhofer SIT-Zertifizierung (vgl. [Fraunhofer BBSec, 2008], S.23). Begründet wird diese Maßnahme allerdings nicht, und untersucht wurde die OTA-Erzeugung des Master Encryption Key auch nicht.*



- b. Es werden keine Identitätsinformationen der Kommunikationsteilnehmer bei der Berechnung des gegenseitigen Bestätigungswertes für den erzeugten geheimen Schlüssel verwendet.
2. **Session-Instanziierung während der Erzeugung des geheimen Schlüssels:** In der gleichen Arbeit weist Tang nach, dass eine Lücke in der o. g. SPEKE-Protokollversion von einem Angreifer ausgenutzt werden kann, um in den Besitz des geheimen Schlüssels zu gelangen, ohne dass die berechtigten Kommunikationsteilnehmer etwas davon bemerken. Voraussetzung für das erfolgreiche Ausnutzen dieser Lücke ist:
- a. Es sind mindestens zwei Instanziierungen der Protokollimplementierung entweder auf der Client- oder der Serverseite gleichzeitig ausführbar.

Darüber hinaus weist Zhao in [Zhao, 2005] darauf hin, dass einige Protokolle der in IEEE P1363.2 vorgeschlagenen EKE-Protokollfamilie anfällig für Offline-Wörterbuchangriffe sind. Zhaos Untersuchungen beziehen sich zwar nicht auf SPEKE, gleichwohl weist er unzureichende Realisierungen von idealen Zahlenmodellen in den ‚Geschwisterprotokollen‘ von SPEKE nach, die zum Verlust der Sicherheit der von ihm untersuchten Protokolle (AuthA, OEKE und SRP¹⁶) führen können.

Im *Key Rollover Protocol*, das das o. g. MQV-Protokoll verwendet, konnten bisher keine Schwächen gefunden werden. Das MQV-Protokoll gilt als sehr sicher.

2.4.2 Mögliche organisatorische Bedrohungen und Schwachstellen

Die entscheidende mögliche organisatorische Bedrohung gegen die OTA-Erzeugung des Master Encryption Keys liegt in der Offenlegung des Wireless Enterprise-Aktivierungspasswortes gegenüber nicht-autorisierten Personen. Sollte dies geschehen, dann kann ein Angreifer, der das Wireless Enterprise-Aktivierungspasswort und zusätzlich die E-Mail-Adresse der von ihm angegriffenen /impersonierten Person kennt, ein BlackBerry-Gerät unautorisiert aktivieren und E-Mails der Person, die er zu sein vorgibt, empfangen oder in ihrem Namen versenden. Dieser Bedrohung kann durch Schwächen bei der Definition oder gar durch Fehlen des Prozesses zur sicheren Verteilung des Aktivierungspassworts Vorschub geleistet werden.

2.5 Bewertung der Bedrohungen und Schwachstellen

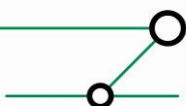
2.5.1 Impersonierung des Servers aus der Sicht des Clients durch einen Angreifer gemäß [Tang, 2005]

Aus Sicht des Autors ist dieser Angriff aus zwei Gründen nicht möglich:

1. Das zwischen BES und dem BlackBerry-Gerät geteilte Geheimnis wird per Definition der BlackBerry Enterprise Activation stets auf im mathematischen Sinn genau zwei Kommunikationsteilnehmer beschränkt: Dieses ist ein definierter BES und ein definierter Benutzer eines Wireless Enterprise Activation-kompatiblen¹⁷ BlackBerry-Geräts. Anders könnte es sein, wenn der BES über eine verteilte und replizierte Benutzerdatenbank (wie dies etwa Active Directory-Domänencontrollern der Fall ist) verfügen würde; dem ist jedoch nicht so.
2. Das in [BB-WEA], S. 10ff beschriebene Verfahren für die Berechnung des Master Encryption Keys fügt Identitätsinformationen der eigenen Seite (BES, bzw. BlackBerry-Gerät) in die Berechnung Bestätigungswertes für den erzeugten geheimen Schlüssel für die andere Seite (BlackBerry-Gerät, bzw. BES) ein. Der von RIM in [BB-WEA], S. 11 als

¹⁶ Mit SRP ist hier das Secure Remote Password Protocol gemeint und nicht das RIM-proprietäre Server Router Protocol; beide Protokolle verwenden dasselbe Akronym.

¹⁷ Vgl. Anmerkung 15.



Enterprise Server key confirmation value bezeichnete Bestätigungswert h_B des BES, den der BES an der das BlackBerry-Gerät schickt, lautet:

$$h_B = \text{HMAC-256}(\text{auxiliary data}_D || \text{auxiliary data}_B || A || B || X || Y || "B")^{18}$$

Dabei fließt in B der Wert des privaten Schlüssels b des BES als Identitätsinformation ein. (Den Wert B des öffentlichen Schlüssels hatte der BES dem BlackBerry-Gerät in einem der ersten Schritte zugesandt.) Analog wird der Bestätigungswert, den das BlackBerry-Gerät an den BES schickt, berechnet.

Damit ist eine Impersonierung nicht möglich.

2.5.2 Session-Instanziierung während der Erzeugung des geheimen Schlüssels gemäß [Tang, 2005]

Nach Tang kann Session-Instanziierung erfolgreich durch die Implementierung einer Session-ID verhindert werden. Diese fließt in den *auxiliary data*_B und *auxiliary data*_D ein. Damit ist ein Angriff über Session-Instanziierung nicht möglich.¹⁹

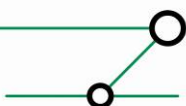
2.5.3 Auswirkung möglicher unzureichender Realisierung von idealen Zahlenmodellen in ‚Geschwisterprotokollen‘ gemäß [Zhao, 2005]

Die von Zhao vorgebrachte Kritik bezieht sich zum einen nicht auf SPEKE, sondern auf die verwandten Protokolle AuthA, OEKE und SRP. Die grundsätzliche Natur seiner Kritik wird von der IEEE 1363-Kommission zur Kenntnis genommen, gleichwohl sind Auswirkungen auf SPEKE bisher nicht bekannt. Die mögliche unzureichende Realisierung von idealen Zahlenmodellen wurde vom Autor dieser Studie erwähnt, weil sie zum einen ein immer wieder auftauchendes Problem der Kryptologie darstellt. Zum anderen könnte sie zusammen mit den von Tang aufgezeigten theoretischen Schwächen bestimmter SPEKE-Implementierungen darauf hindeuten, dass möglicherweise weitere Schwächen in SPEKE aufgedeckt werden könnten. Gleichwohl gilt es festzuhalten, dass derzeit keinerlei Auswirkungen von Zhaos Untersuchung auf die Implementierung von SPEKE in der BlackBerry Enterprise Software festzustellen sind.

¹⁸ Dabei fließt in X das über ECC von dem BlackBerry-Gerät behandelte an den Benutzer out-of-Band zu verteilende Passwort ein, in Y das von dem BES analog behandelte Passwort, in *auxiliary data*_D fließen eine Transaktions-ID, Netzwerk-Daten und weitere BlackBerry-spezifische Daten ein, analog fließen *auxiliary data*_B in zusätzliche und teilweise BES-spezifische Daten ein. Das Zeichen $||$ steht für Konkatenation als eine definierte Form der bitweisen Verknüpfung. Die genauen Definitionen entnimmt man [BB-WEA], S. 10f.

¹⁹ Unabhängig davon ist dem Autor keine Möglichkeit bekannt, mehr als eine Instanz eines spezifischen Aktivierungsprozesses gleichzeitig entweder auf dem BlackBerry-Gerät oder dem BES auszuführen. Doch selbst wenn dies möglich sein sollte, verhindert die integrierte Session-ID einen erfolgreichen Angriff über Session-Instanziierung. Der Verfasser dieser Studie wandte sich mit den in Abschnitt 2.3.1 aufgeführten möglichen technischen Bedrohungen und Schwachstellen und der in Abschnitt 2.4 dargestellten Bewertung dieser Bedrohungen und Schwachstellen an die Security-Abteilung von RIM mit der Bitte um eine Stellungnahme. In der schriftlichen Stellungnahme bestätigte RIM dem Verfasser, dass weder Impersonierung noch Session-Instanziierung möglich sind.

Definition – Umsetzung – Kontrolle



2.6 Bereits implementierte Schutzmaßnahmen

Von RIM wurden weitere Schutzmaßnahmen zur OTA-Erzeugung des Master Encryption Keys sowie des Wireless Enterprise-Aktivierungspasswortes implementiert. Diese sind:

- Das Wireless Enterprise-Aktivierungspasswort kann nach seiner Setzung am BES nur für 48 Stunden genutzt werden, danach verfällt es und kann nicht mehr benutzt werden.
- Ein einmal verwendetes Wireless Enterprise-Aktivierungspasswort kann nicht wieder /nicht für eine weitere Aktivierung verwendet werden.
- Nach fünf fehlerhaften Eingaben ist das Aktivierungspasswort nicht mehr verwendbar. Es muss ein neues Aktivierungspasswort von dem Administrator des BES gesetzt werden.
- FIPS 140-2 zertifizierte Kryptomodule in der BlackBerry Enterprise Software zusammen mit dem MQV-Protokoll sorgen für die OTA-Erzeugung eines neuen (ab dem zweiten) Master Encryption Key zwischen BlackBerry-Gerät und BES.
- Automatische Neuerzeugung eines Master Encryption Key zwischen BlackBerry-Gerät und BES nach spätestens 30 Tagen mit der Möglichkeit die Neuerzeugung sowohl auf dem BES als auch auf dem BlackBerry-Gerät innerhalb kürzerer Zeit zu initiieren.

2.7 Zusätzlich empfohlene Schutzmaßnahmen

Zum Schutz der OTA-Erzeugung des Master Encryption Keys im Sinne dieser Studie gibt es zwei zusätzliche Empfehlungen:

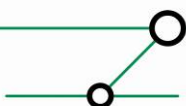
1. Es sollte eine Policy definiert werden, die einen sicheren Prozess der Wireless Enterprise Activation vorschreibt. In dieser Policy sollte u. a. Folgendes definiert sein:
 - a. Welche Benutzer mit welchen BlackBerry-Geräten für die Wireless Enterprise Activation zugelassen sind.
 - b. Für diesen Prozess verantwortlicher BES-Administrator.
 - c. Wie die Out-of-the-Band-Vergabe des Aktivierungspasswortes erfolgt.
 - d. Passworrichtlinie für das Aktivierungspasswort.²⁰
2. Es sollte möglichst bald nach der Aktivierung die Erzeugung eines neuen Master Encryption Keys über das *Key Rollover Protocol* initiiert werden. (Auch diese Maßnahme kann in der Wireless Enterprise Activation-Policy beschrieben werden.)

Weiterhin empfiehlt der Autor die Aktivierung der sog. *Content Protection* zum Schutz der auf einem BlackBerry-Gerät gespeicherten Daten. Dann können sowohl die Daten als auch der Master Encryption Key sowie andere Schlüssel verschlüsselt gespeichert werden, wenn das BlackBerry-Gerät gesperrt ist. Dazu sollte die Policy, *Content Protection Strength IT-Policy*²¹, gesetzt werden: empfohlen wird der Wert *Stronger*, damit ein 283-bit ECC-Schlüssel für die Verschlüsselung der gespeicherten Daten verwendet wird. Zusätzlich muss die *Password Required IT-Policy* gesetzt werden. Da der Schlüssel, der den 256-bit AES Content-Protection-Schlüssel sowie den privaten 283-bit ECC-Schlüssel verschlüsselt, von der Güte des BlackBerry-Gerätepassworts abhängt, sollte die *Minimum Password Length IT-Policy* auf mindestens zwölf Zeichen gesetzt werden. Die in diesem Absatz genannten Empfehlungen berühren zwar nicht die OTA-Erzeugung von Master Encryption Keys, sie stellen jedoch flankierende Schutzmaßnahmen dar, die sowohl den Prozess der Wireless Enterprise Activation als auch den Prozess des Master Encryption Key-Updates in einen sicheren Gesamtkontext einbetten²².

²⁰ Randbedingungen für mögliche Werte entnimmt man [BB-WEA], S. 2.

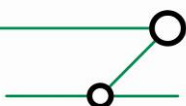
²¹ Sämtliche hier genannten Policies finden sich detailliert beschrieben in [BB-PRG].

²² Eine gute Sammlung von technischen und organisatorischen Schutzmaßnahmen findet sich in [DISA, 2007].



2.8 Fazit

Die Erzeugung von Master Encryption Keys zur Inbetriebnahme von BlackBerry-Geräten und für das automatische Update von Master Encryption Keys zwischen BlackBerry-Geräten und dem BlackBerry Enterprise Server (BES) wird aufgrund der vorliegenden Untersuchung als sicher im Sinne aktueller Sicherheitsstandards bewertet. Dies gilt für die Erzeugung von Master Encryption Keys über die BlackBerry Desktop Software, und es gilt auch für die OTA-Erzeugung von Master Encryption Keys, **wenn** die OTA-Erzeugung von einer Policy begleitet wird, die die organisatorischen Aspekte der OTA-Erzeugung im Sinne der in dieser Untersuchung empfohlenen Schutzmaßnahmen beinhaltet, und wenn die zugrunde liegenden Betriebssystem- und Mailserverkonfigurationen im Sinne aktueller Best Practices durchgeführt werden. In diesem Fall sind beide Methoden zur Erzeugung von Master Encryption Keys sowohl technisch als auch organisatorisch als sicher zu betrachten.



3 QUELLEN

- [@Stake, 2003]: @stake, BlackBerry by Research in Motion: An @stake Security Assessment, 2003, http://www.vodafone.co.nz/business/blackberry/an_at_stake_security_assessment.pdf
- [A-SIT, 2004]: Zentrum für sichere Informationstechnologie Austria, Sicherheitsanalyse BlackBerry Mobile Data Services, 2004, <http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19390>
- [BB-PRG]: Policy Reference Guide. Version 28. BlackBerry Enterprise Server, <http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=6199802&sliceId=&dialogID=199430550&stateId=0095305393>
- [BB-STO]: BlackBerry Enterprise Solution Security. Technical Overview for BlackBerry Enterprise Server 4.1 Service Pack 5 and BlackBerry Device Software Version 4.5, http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/1272812/1272762/BlackBerry_Enterprise_Solution_Version_4.1.2_Security_Technical_Overview?nodeid=1272692&vernum=0
- [BB-WEA]: BlackBerry Wireless Enterprise Activation. Technical Overview. Release 4.0, http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/BlackBerry_Wireless_Enterprise_Activation_Technical_White_Paper.pdf?nodeid=1181988
- [DISA, 2007]: Defense Information Systems Agency (DISA), Wireless STIG BlackBerry Security Checklist Version 5 Release 2.1, http://iase.disa.mil/stigs/checklist/wireless_stig_blackberry_checklist_v5r2-1.pdf
- [ERNW, 2006]: Dror-John Roecher, BlackBerry & Mobile Security, in: ERNW-Newsletter 11/2006, http://www.ernw.de/content/e15/e28/e65/download67/ERNW_Newsletter_11_de_ger.pdf
- [Fraunhofer, 2006]: Corporate Statement von RIM vom 11. September 2006, http://www.sit.fraunhofer.de/fhg/Images/060911_RIM_Statement_DE_tcm105-102418.pdf
- [Fraunhofer BBSec, 2008]: Fraunhofer SIT, BlackBerry Enterprise Solution for Microsoft Exchange Security Analysis, http://testlab.sit.fraunhofer.de/downloads/certificates/Certification_Report-06-104302.pdf
- [IEE1363.2]: IEE1363.2 /D28 Draft Standard for Specifications for Password based Public Key Cryptographic Techniques (Revision of IEEE 1363-2000), 2007, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=4383571&anumber=4383572&punumber=4383570
- [ISO11770-4]: ISO/IEC 11770-4 Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39723
- [RIM, 2008]: Matthias Dosch, Sicherheit der BlackBerry Enterprise Lösung, http://www.inmac.de/inmac_assets/it_symposium/vortraege2008/Inmac_IT_Symposium_BlackBerry.pdf
- [Secorvo, 2005]: Dirk Fox, Das Sicherheitskonzept des E-Mail-Push-Dienstes BlackBerry, v1.0 2005, in Secorvo White Paper, <http://www.secorvo.de/whitepapers/secorvo-wp12.pdf>
- [SP800-56A]: NIST Special Publication 800-56A, Elaine Barker et al., Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2007, http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf
- [Tang, 2005]: Quing Tang et al., On the security of some password-based key agreement schemes, 2005, <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.1522>
- [Vanstone, 2005], Deployments of Elliptic Curve Cryptography, 2005, <http://www.cacr.math.uwaterloo.ca/conferences/2005/ecc2005/vanstone.pdf>



[Zhao, 2005]: Zhu Zhao et al., Security analysis of a password-based authentication protocol proposed to IEEE 1363, 2005,
<http://portal.acm.org/citation.cfm?id=1142859.1142880&coll=GUIDE&dl=GUIDE>

Für weitere Fragen steht Ihnen das Team von **ERNW-Deutschland** und **ERNW-Portugal** gern zur Verfügung.

Mit freundlichen Grüßen,

Friedwart Kuhn.

ERNW GmbH
Friedwart Kuhn
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 15152411855
Mobil (Portugal): +351 91 8763637
www.ernw.de

