



S/MIME Support Package für BlackBerry-Geräte

Benutzerhandbuchzusatz

BlackBerry Pearl 8120-Smartphone

BlackBerry Pearl 8130-Smartphone

S/MIME Support Package für BlackBerry-Geräte Benutzerhandbuchzusatz

Zuletzt geändert am: 20. Juli 2007

Dokument-ID: 13381054-003

Zum Zeitpunkt der Veröffentlichung basiert die vorliegende Dokumentation auf dem S/MIME Support Package für BlackBerry-Geräte Version 4.3.

Senden Sie uns Ihre Kommentare zur Produktdokumentation: <https://www.blackberry.com/DocsFeedback>.

Inhalt

| | | |
|---|---|----|
| 1 | Installieren des S/MIME Support Package für BlackBerry-Geräte | 5 |
| 2 | Zertifikate | 7 |
| 3 | Zertifikatsserver | 17 |
| 4 | S/MIME-Nachrichten | 19 |
| 5 | Smart Cards..... | 29 |
| 6 | Rechtliche Hinweise | 35 |

Installieren des S/MIME Support Package für BlackBerry-Geräte

Info zum S/MIME Support Package für BlackBerry-Geräte

Installieren Sie das Tool für die Zertifikats-synchronisierung auf Ihrem Computer.

Voraussetzungen für das S/MIME Support Package für BlackBerry-Geräte

Installieren des S/MIME Support Package für BlackBerry-Geräte auf Ihrem Computer

Installieren des S/MIME Support Package für BlackBerry-Geräte auf Ihrem BlackBerry-Gerät

Info zum S/MIME Support Package für BlackBerry-Geräte

Das S/MIME Support Package für BlackBerry®-Geräte wurde entwickelt, um Ihnen das Verschieben und Empfangen von S/MIME-(Secure Multipurpose Internet Mail Extensions-)Nachrichten von Ihrem Gerät zu ermöglichen, wenn Sie diese Art von Nachrichten bereits über Ihren Computer verschicken und empfangen.

Installieren Sie das Tool für die Zertifikats-synchronisierung auf Ihrem Computer.

1. Legen Sie die *BlackBerry User Tools* CD in Ihr Laufwerk ein.
2. Folgen Sie den Anweisungen auf dem Bildschirm.

3. Führen Sie im Fenster zur Programmverwaltung oder für den Installationstyp eine der folgenden Aktionen aus:
 - Wählen Sie bei der Neuinstallation der BlackBerry® Desktop Software im Fenster „Installationstyp“ die Option **Benutzerdefiniert**.
 - Wenn Sie die BlackBerry Desktop Software durch das Tool für die Zertifikats-synchronisierung erweitern möchten, wählen Sie im Fenster für die Programmverwaltung die Option **Ändern**.
4. Klicken Sie auf **Zertifikatsynchronisierung**.
5. Klicken Sie auf die **Option zur Installation dieser Funktion und aller dazugehörigen Funktionen auf der lokalen Festplatte**.

Informationen zur Verwendung des Tools für die Zertifikatsynchronisierung erhalten Sie in der *Online-Hilfe zur BlackBerry Desktop Software*.

Voraussetzungen für das S/MIME Support Package für BlackBerry-Geräte

- Überprüfen Sie, ob auf Ihrem Computer die BlackBerry® Device Software installiert ist. Für die Installation des S/MIME Support Package für BlackBerry-Geräte werden einzelne Komponenten der BlackBerry Device Software benötigt.
- Vergewissern Sie sich, dass Sie über das Installationsprogramm für das S/MIME Support Package für BlackBerry-Geräte verfügen.

Installieren des S/MIME Support Package für BlackBerry-Geräte auf Ihrem Computer

1. Doppelklicken Sie auf das Installationssymbol für das S/MIME Support Package für BlackBerry®-Geräte.
2. Folgen Sie den Anweisungen auf dem Bildschirm.

Installieren des S/MIME Support Package für BlackBerry-Geräte auf Ihrem BlackBerry-Gerät

1. Schließen Sie Ihr BlackBerry®-Gerät an einen Computer an.
2. Klicken Sie in der Taskleiste auf **Start > Programme > BlackBerry > Desktop Manager**.
3. Doppelklicken Sie auf das Symbol **Programm zum Laden von Anwendungen**.
4. Klicken Sie auf **Weiter**.
5. Aktivieren Sie das Kontrollkästchen **BlackBerry S/MIME Support Package**.
6. Wenn Sie Stammzertifikate des Department of Defense (DoD, amerikanisches Verteidigungsministerium) benötigen, aktivieren Sie das **entsprechende Kontrollkästchen**.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.

Verwandte Themen

[Rechtliche Hinweise \(Siehe Seite 35.\)](#)

Zertifikate

Info über Zertifikate
Info über Zertifikatssymbole
Herunterladen eines Zertifikats
Filtern von Zertifikaten
Anzeigen von Zertifikatinformationen
Felder mit Zertifikatinformationen
Suchen von Zertifikaten in einer Kette
Überprüfen des Status eines Zertifikats oder einer Zertifikatskette
Festlegen des Status eines Zertifikats auf vertrauenswürdig
Festlegen des Status eines Zertifikats auf nicht vertrauenswürdig
Senden eines Zertifikats an einen Ansprechpartner
Hinzufügen einer E-Mail-Verknüpfung zu einem Zertifikat
Einstellen der Optionen zur Überprüfung des Zertifikatsstatus
Verwenden des gebräuchlichen Namens bei Hinzufügen eines Zertifikats zum Schlüsselspeicher
Ändern des Anzeigenamens für ein Zertifikat
Ändern der Sicherheitsstufe für einen privaten Schlüssel
Sperren eines Zertifikats
Widerrufsgründe
Löschen eines Zertifikats
Hinzufügen eines Ansprechpartners, wenn dem Schlüsselspeicher ein Zertifikat hinzugefügt wird

Festlegen des Dienstes zum Herunterladen von Zertifikaten
Ablehnen von CRLs von nicht verifizierten Zertifikatservern
Info zum Schlüsselspeicher
Ändern des Kennworts für den Schlüsselspeicher
Einstellen der Speicherdauer Ihres Schlüsselspeicher-Kennworts
Einstellen der Aktualisierungshäufigkeit des Widerrufstatus
Informationen im Schlüsselspeicher nicht sichern oder wiederherstellen
Tastenkombinationen zum Filtern von Zertifikaten
Tastenkombinationen zum Anzeigen von Zertifikatinformationen
Fehlerbehebung für Zertifikate

Info über Zertifikate

Ein Zertifikat ist ein digitales Dokument, das die Identität und den öffentlichen Schlüssel eines Zertifikatempfängers verbindet. Jedem Zertifikat ist ein privater Schlüssel zugeordnet. Zertifikate können Sie bei einer Zertifizierungsstelle anfordern. Diese signiert die Zertifikate und bescheinigt so ihre Glaubwürdigkeit.

Andere Benutzer verschlüsseln dann mit Hilfe des öffentlichen Schlüssels Ihres Zertifikats E-Mails an Sie. Erhalten die Benutzer E-Mails von Ihnen, überprüfen sie damit deren Signatur. Ihr BlackBerry®-Gerät verwendet den privaten Schlüssel Ihres Zertifikats zum Signieren von versendeten und zum Entschlüsseln von eingegangenen E-Mails. Informationen zum privaten Schlüssel sind niemals öffentlich verfügbar.

Verwandte Themen

[Info über Zertifikatssymbole \(Siehe Seite 8.\)](#)

[Info über digitale Signaturen und Verschlüsselung \(Siehe Seite 19.\)](#)

[Info zum Schlüsselspeicher \(Siehe Seite 14.\)](#)

Info über Zertifikatssymbole

Folgende Symbole zeigen den Status der Zertifikate an, die auf Ihrem BlackBerry®-Gerät gespeichert sind:

- **Schlüssel:** Für das Zertifikat liegt ein entsprechender privater Schlüssel auf Ihrem Gerät oder einer Smartcard vor.
- **Häkchen:** Die Zertifikatskette ist vertrauenswürdig, ihr Widerrufstatus und die Zertifikatskette selbst sind gültig.
- **Fragezeichen:** Der Widerrufstatus der Zertifikatskette ist unbekannt oder ein öffentlicher Schlüssel in der Zertifikatskette ist schwach.
- **X:** Die Zertifikatskette ist nicht glaubwürdig, noch nicht gültig oder abgelaufen, sie wurde widerrufen oder konnte nicht verifiziert werden.

Herunterladen eines Zertifikats

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Drücken Sie die **Menütaste**.
4. Klicken Sie auf **Zertifikate abrufen**.

5. Wählen Sie einen LDAP-Server (Lightweight Directory Access Protocol) aus.
6. Geben Sie für den Zertifikatempfänger Daten in eines oder mehrere der Felder **Vorname**, **Nachname** oder **E-Mail** ein.
7. Drücken Sie die **Menütaste**.
8. Klicken Sie auf **Suchen**.
9. Klicken Sie auf ein Zertifikat mit nicht aktiviertem Kontrollkästchen.
10. Klicken Sie auf **Zertifikat zu Schlüsselspeicher hinzufügen**.
11. Geben Sie Ihr Kennwort für den Schlüsselspeicher ein.
12. Klicken Sie auf **OK**.

Ein aktiviertes Kontrollkästchen neben einem Zertifikat zeigt an, dass dieses Zertifikat im Schlüsselspeicher Ihres BlackBerry®-Geräts gespeichert ist.

Hinweis:

Ihr Gerät fordert Sie möglicherweise auf, den Zertifikatsstatus herunterzuladen oder eine Bezeichnung für das Zertifikat einzugeben.

Verwandte Themen

[Info zum Schlüsselspeicher \(Siehe Seite 14.\)](#)

[Einstellen der Optionen zur Überprüfung des Zertifikatsstatus \(Siehe Seite 11.\)](#)

[Verwenden des gebräuchlichen Namens bei Hinzufügen eines Zertifikats zum Schlüsselspeicher \(Siehe Seite 12.\)](#)

[Das Herunterladen eines Zertifikats funktioniert nicht \(Siehe Seite 16.\)](#)

Filtern von Zertifikaten

Der aktuelle Filter wird in der oberen rechten Ecke des Bildschirms angezeigt.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Drücken Sie die **Menütaste**.
4. Führen Sie eine der folgenden Aktionen aus:
 - Zum Anzeigen aller Zertifikate auf Ihrem BlackBerry®-Gerät klicken Sie auf **Alle Zertifikate anzeigen**.
 - Zum Anzeigen Ihrer Zertifikate klicken Sie auf **Meine Zertifikate anzeigen**.
 - Zum Anzeigen der Zertifikate anderer Benutzer klicken Sie auf **Sonstige Zertifikate anzeigen**.
 - Zum Anzeigen der Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) klicken Sie auf **CA-Zertifikate anzeigen**.
 - Zum Anzeigen der Stammzertifikate der Zertifizierungsstelle klicken Sie auf **Stammzertifikate anzeigen**.

Verwandte Themen

Tastenkombinationen zum Filtern von Zertifikaten
(Siehe Seite 15.)

Anzeigen von Zertifikatinformationen

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Klicken Sie auf ein Zertifikat.

Verwandte Themen

Suchen von Zertifikaten in einer Kette (Siehe Seite 10.)

Ändern des Anzeigenamens für ein Zertifikat (Siehe Seite 12.)

Tastenkombinationen zum Anzeigen von Zertifikatinformationen (Siehe Seite 16.)

Felder mit Zertifikatinformationen

- **Widerrufsstatus:** Der Status eines Zertifikats zu einem festgelegten Datum und einer festgelegten Uhrzeit.
- **Vertrauensstatus:** Die Vertrauenswürdigkeit eines Zertifikats.
 - **Sehr vertrauenswürdig:** Das Zertifikat selbst ist vertrauenswürdig.
 - **Indirekt vertrauenswürdig:** Das Zertifikat ist mit einem Zertifikat auf Ihrem BlackBerry®-Gerät verbunden, das vertrauenswürdig ist.
 - **Nicht vertrauenswürdig:** Das Zertifikat ist nicht vertrauenswürdig und nicht mit einem vertrauenswürdigem Zertifikat auf Ihrem Gerät verbunden.
- **Ablaufdatum:** Das von der ausgebenden Zertifizierungsstelle (Certificate Authority, CA) festgelegte Ablaufdatum.
- **Zertifikatstyp:** Das PKI-Zertifikatsformat (Public Key Infrastructure).
- **Typ des öffentlichen Schlüssels:** Standard, dem der öffentliche Schlüssel entspricht. Ihr Gerät unterstützt die Schlüssel RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm, digitaler Signaturalgorithmus), DH (Diffie-Hellman) und ECC (Elliptic Curve Cryptography, Kryptographieverfahren basierend auf elliptischer Kurve).
- **Empfänger:** Detaillierte Informationen über den Zertifikatempfänger.
- **Aussteller:** Detaillierte Informationen zum Aussteller eines Zertifikats.
- **Seriennummer:** Die Seriennummer des Zertifikats im Hexadezimalformat.
- **Schlüsselverwendung:** Genehmigte Einsatzzwecke für den Schlüssel.
- **Alternativname Zertifikatempfänger:** Die E-Mail-Adresse für ein Zertifikat, falls bekannt.

- **SHA1-Fingerabdruck:** Der digitale Fingerabdruck Secure Hash Algorithm, Version 1 (SHA1), eines Zertifikats.
- **MD5-Fingerabdruck:** Der digitale Fingerabdruck Message-Digest-Algorithm, Version 5 (MD5), eines Zertifikats.

Verwandte Themen

[Info über Zertifikate \(Siehe Seite 7.\)](#)

[Anzeigen von Zertifikatinformationen \(Siehe Seite 9.\)](#)

Suchen von Zertifikaten in einer Kette

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Kette anzeigen**.

Verwandte Themen

[Anzeigen von Zertifikatinformationen \(Siehe Seite 9.\)](#)

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Führen Sie eine der folgenden Aktionen aus:
 - Zum Verifizieren des Status eines Zertifikats klicken Sie auf **Status abrufen**.
 - Zum Verifizieren des Status eines Zertifikats und aller anderen Zertifikate einer Kette klicken Sie auf **Kettenstatus abrufen**.

Verwandte Themen

[Info zum Schlüsselspeicher \(Siehe Seite 14.\)](#)

[Herunterladen eines Zertifikats \(Siehe Seite 8.\)](#)

Festlegen des Status eines Zertifikats auf vertrauenswürdig

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat mit nicht vertrauenswürdigem Status.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Vertrauenswürdigkeit**.
6. Wenn das Zertifikat kein Stammzertifikat ist, wird eine Eingabeaufforderung angezeigt. Führen Sie eine der folgenden Aktionen aus:
 - Um ausschließlich das markierte Zertifikat als vertrauenswürdig einzustufen, klicken Sie auf **Ausgewähltes Zertifikat**.
 - Um die gesamte Zertifikatskette durch Bestätigen des Stammzertifikats als vertrauenswürdig einzustufen, klicken Sie auf **Ganze Kette**.

Verwandte Themen

[Info über Zertifikate \(Siehe Seite 7.\)](#)

[Info über Zertifikatssymbole \(Siehe Seite 8.\)](#)

[Festlegen des Status eines Zertifikats auf nicht vertrauenswürdig \(Siehe Seite 10.\)](#)

Festlegen des Status eines Zertifikats auf nicht vertrauenswürdig

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein vertrauenswürdiges Zertifikat.

4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Nicht vertrauen**.

Verwandte Themen

[Info über Zertifikate \(Siehe Seite 7.\)](#)

[Info über Zertifikatssymbole \(Siehe Seite 8.\)](#)

Senden eines Zertifikats an einen Ansprechpartner

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Über E-Mail senden** oder **Über PIN senden**.

Hinweis:

Wenn Sie ein Zertifikat verschicken, wird lediglich der öffentliche, nicht aber der private Schlüssel verschickt.

Verwandte Themen

[Anfügen eines Zertifikats an eine Nachricht \(Siehe Seite 24.\)](#)

[Importieren eines Zertifikats aus einer Nachricht \(Siehe Seite 21.\)](#)

Hinzufügen einer E-Mail-Verknüpfung zu einem Zertifikat

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie das Zertifikat eines anderen Benutzers.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Verknüpfte Adressen**.
6. Klicken Sie mit dem Trackball.

7. Klicken Sie auf **Adresse hinzufügen**.
8. Klicken Sie auf **[Einmalig]**.
9. Geben Sie eine E-Mail-Adresse ein.
10. Klicken Sie mit dem Trackball.
11. Drücken Sie die **Menütaste**.
12. Klicken Sie auf **Speichern**.

Zum Löschen der verknüpften Adresse klicken Sie zunächst auf die Adresse. Klicken Sie dann auf **Adresse löschen**.

Verwandte Themen

[Info zum Schlüsselspeicher \(Siehe Seite 14.\)](#)

[Filtern von Zertifikaten \(Siehe Seite 8.\)](#)

Einstellen der Optionen zur Überprüfung des Zertifikatsstatus

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Drücken Sie die **Menütaste**.
4. Klicken Sie auf **Zertifikate abrufen**.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Optionen**.
7. Führen Sie eine der folgenden Aktionen aus:
 - Nehmen Sie im Feld **Status abrufen** die Einstellung **Ja** vor, um den Zertifikatsstatus immer dann abzurufen, wenn Sie ein Zertifikat zum Schlüsselspeicher hinzufügen.
 - Nehmen Sie im Feld **Status abrufen** die Einstellung **Eingabeaufforderung** vor, um den Zertifikatsstatus immer dann abzurufen, wenn Sie ein Zertifikat zum Schlüsselspeicher hinzufügen.
 - Nehmen Sie im Feld **Status abrufen** die Einstellung **Nein** vor, um den Zertifikatsstatus nie abzurufen, wenn Sie ein Zertifikat zum Schlüsselspeicher hinzufügen.

8. Drücken Sie die **Menütaste**.
9. Klicken Sie auf **Speichern**.

Verwandte Themen

Info zum Schlüsselspeicher (Siehe Seite 14.)

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette (Siehe Seite 10.)

Verwenden des gebräuchlichen Namens bei Hinzufügen eines Zertifikats zum Schlüsselspeicher

Der gebräuchliche Name ist der bei der Erstellung des Schlüssels vergebene Name. Sie können als Bezeichnung für den Schlüssel auf Ihrem BlackBerry®-Gerät entweder den gebräuchlichen Namen verwenden oder einen Namen, der für Sie aussagekräftiger ist.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Drücken Sie die **Menütaste**.
4. Klicken Sie auf **Zertifikate abrufen**.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Optionen**.
7. Legen Sie für das Feld **Bezeichnung fordern** die Einstellung **Nein** fest.
8. Drücken Sie die **Menütaste**.
9. Klicken Sie auf **Speichern**.

Verwandte Themen

Ändern des Anzeigenamens für ein Zertifikat (Siehe Seite 12.)

Hinzufügen eines Ansprechpartners, wenn dem Schlüsselspeicher ein Zertifikat hinzugefügt wird (Siehe Seite 13.)

Ändern des Anzeigenamens für ein Zertifikat

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Bezeichnung ändern**.
6. Geben Sie ein neues Zertifizierungsetikett ein.
7. Klicken Sie auf **OK**.

Verwandte Themen

Verwenden des gebräuchlichen Namens bei Hinzufügen eines Zertifikats zum Schlüsselspeicher (Siehe Seite 12.)

Ändern der Sicherheitsstufe für einen privaten Schlüssel

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein persönliches Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Sicherheitsstufe ändern**.
6. Drücken Sie zum Ändern der **Sicherheitsstufe** die **Leertaste**.
7. Klicken Sie auf **OK**.

Sperrung eines Zertifikats

Wenn Sie ein Zertifikat widerrufen, ist es nur im Schlüsselspeicher Ihres BlackBerry®-Geräts gesperrt, die Sperrung wird nicht an die Zertifizierungsstelle (CA) oder die CRL-Server (Certificate Revocation List, Liste ungültiger Zertifikate) weitergegeben.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.

2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Sperren**.
6. Klicken Sie auf **Ja**.
7. Drücken Sie die **Leertaste**, um das Feld **Grund** auf den entsprechenden Grund für den Widerruf einzustellen.
8. Klicken Sie auf **OK**.

Wenn Sie das Feld „Grund“ auf die Einstellung „Vorläufige Sperrung“ setzen, um das Zertifikat wieder einzusetzen, markieren Sie das Zertifikat. Drücken Sie die **Menütaste**. Klicken Sie auf **Vorläufige Sperrung abbrechen**.

Verwandte Themen

Widerrufsgründe (Siehe Seite 13.)

Info zum Schlüsselspeicher (Siehe Seite 14.)

Festlegen des Status eines Zertifikats auf nicht vertrauenswürdig (Siehe Seite 10.)

Löschen eines Zertifikats (Siehe Seite 13.)

Widerrufsgründe

- **Unbekannt:** Der Grund wurde nicht genauer angegeben.
- **Schlüsselkompromittierung:** Anderen Personen als dem Schlüsselhalter wurde möglicherweise der Wert des privaten Schlüssels bekannt.
- **CA-Kompromittierung:** Der ausgebende private Schlüssel der Zertifizierungsstelle (CA) ist möglicherweise bekannt.
- **Änderung bei Zugehörigkeit:** Die Person ist nicht mehr im Unternehmen tätig.
- **Ersetzt:** Ein bestehendes Zertifikat wird durch ein neues ersetzt.
- **Betrieb eingestellt:** Das Zertifikat ist nicht mehr erforderlich.

- **Vorläufige Sperrung:** Das Zertifikat ist vorübergehend gesperrt.
- **Aus CRL entfernen:** Das gesperrte Zertifikat wird aus der CRL (Certificate Revocation List (Liste ungültiger Zertifikate)) entfernt.

Verwandte Themen

Sperren eines Zertifikats (Siehe Seite 12.)

Löschen eines Zertifikats

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikate**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Löschen**.

Verwandte Themen

Sperren eines Zertifikats (Siehe Seite 12.)

Festlegen des Status eines Zertifikats auf nicht vertrauenswürdig (Siehe Seite 10.)

Hinzufügen eines Ansprechpartners, wenn dem Schlüsselspeicher ein Zertifikat hinzugefügt wird

Sie können Ihrem Adressbuch automatisch neue Ansprechpartner von Zertifikaten hinzufügen, wenn Sie dem Schlüsselspeicher Ihres BlackBerry®-Geräts ein Zertifikat hinzufügen.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.
3. Legen Sie für das Feld **Adresseninjektor des Schlüsselspeichers** die Option **Aktiviert** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

[Info zum Schlüsselspeicher \(Siehe Seite 14.\)](#)

Festlegen des Dienstes zum Herunterladen von Zertifikaten

Prüfen Sie, ob Ihr Systemadministrator Ihnen den Service-Datensatz für den BlackBerry MDS™ Connection Service (BlackBerry Mobile Data System™), den Verbindungsdienst von BlackBerry, zur Verfügung gestellt hat, mit dem Ihr BlackBerry®-Gerät Zertifikate herunterlädt.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.
3. Stellen Sie das Feld **Zertifikatdienst** auf den korrekten Service-Datensatz ein.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

[Herunterladen eines Zertifikats \(Siehe Seite 8.\)](#)

Ablehnen von CRLs von nicht verifizierten Zertifikatservern

Wenn Sie CRLs (Certificate Revocation List (Liste ungültiger Zertifikate)) von nicht verifizierten Zertifikatservern ablehnen, akzeptiert Ihr BlackBerry®-Gerät keine Zertifikatsstatusmeldungen von CRLs, die nicht vom BlackBerry MDS™ Connection Service (BlackBerry Mobile Data System™) verifiziert werden können.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.
3. Nehmen Sie im Feld **Nicht verifizierte CRLs annehmen** die Einstellung **Nein** vor.
4. Drücken Sie die **Menütaste**.

5. Klicken Sie auf **Speichern**.

Verwandte Themen

[Festlegen des Dienstes zum Herunterladen von Zertifikaten \(Siehe Seite 14.\)](#)

Info zum Schlüsselspeicher

Der Schlüsselspeicher auf Ihrem BlackBerry®-Gerät speichert folgende Informationen:

- persönliche Zertifikate (Zertifikate und private Schlüsselpaare)
- Zertifikate, die vom Tool für die Zertifikats-synchronisierung im BlackBerry Desktop Manager heruntergeladen wurden
- Zertifikate, die von einem LDAP-Server (Lightweight Directory Access Protocol) heruntergeladen wurden
- aus einer Nachricht importierte Zertifikate
- Stammzertifikate, die mit BlackBerry Desktop Software gebündelt sind

Der Schlüsselspeicher ist durch ein Schlüsselspeicher-Kennwort geschützt. Ihr Gerät fordert Sie beim ersten Öffnen des Schlüsselspeichers zur Einrichtung eines Schlüsselspeicher-Kennwortes auf. Dieses Kennwort benötigen Sie, um Schlüssel hinzuzufügen oder aus dem Schlüsselspeicher zu löschen, oder wenn eine Anwendung versucht, auf Ihren privaten Schlüssel zuzugreifen, um eine Nachricht zu signieren oder zu entschlüsseln.

Verwandte Themen

[Herunterladen eines Zertifikats \(Siehe Seite 8.\)](#)

Ändern des Kennworts für den Schlüsselspeicher

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.

3. Drücken Sie die **Menütaste**.
4. Klicken Sie auf **Kennwort ändern**.

Verwandte Themen

Info zum Schlüsselspeicher (Siehe Seite 14.)

Einstellen der Speicherdauer Ihres Schlüsselspeicher-Kennworts (Siehe Seite 15.)

Einstellen der Speicherdauer Ihres Schlüsselspeicher-Kennworts

Wenn ein Kennwort-Timeout eintritt, müssen Sie Ihr Kennwort eingeben, um auf private Schlüssel zuzugreifen.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.
3. Geben Sie im Feld **Timeout für das Kennwort des privaten Schlüssels** einen Wert ein.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Info zum Schlüsselspeicher (Siehe Seite 14.)

Ändern des Kennworts für den Schlüsselspeicher (Siehe Seite 14.)

Einstellen der Aktualisierungshäufigkeit des Widerrufstatus

Speichert Ihr BlackBerry®-Gerät ein Zertifikat länger als die im Feld „Zertifikatsstatus läuft ab nach:“ vorgegebene Dauer, lädt Ihr Gerät beim nächsten Einsatz des Zertifikats automatisch einen neuen Widerrufstatus herunter.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.

3. Geben Sie im Feld **Zertifikatsstatus läuft ab nach**: eine Zeitdauer ein, während der ein Widerrufstatus gespeichert wird, ehe Ihr Gerät den Status als nicht mehr aktuell bewertet.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette (Siehe Seite 10.)

Informationen im Schlüsselspeicher nicht sichern oder wiederherstellen

Im Feld „Sicherung/Wiederherstellung des Schlüsselspeichers zulassen“ können Sie festlegen, ob die Informationen im Schlüsselspeicher bei Sicherung oder Wiederherstellung Ihres BlackBerry®-Gerätes gesichert oder wiederhergestellt werden. Die Schlüssel sind auf Ihrem Computer zwar verschlüsselt, dennoch wird aus Sicherheitsgründen empfohlen, die Einstellung „Nein“ vorzunehmen, damit Ihr privater Schlüssel nicht auf Ihrem Computer gespeichert wird.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Schlüsselspeicher**.
3. Wählen Sie für das Feld **Sicherung/Wiederherstellung des Schlüsselspeichers zulassen** die Einstellung **Nein**.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Info zum Schlüsselspeicher (Siehe Seite 14.)

Tastenkombinationen zum Filtern von Zertifikaten

Zum Anzeigen aller Zertifikate drücken Sie die **Alt-Taste** und das **Fragezeichen (?)**.

Zum Anzeigen der Zertifizierungsstelle (CA) drücken Sie die **Alt-Taste** und die **7**.

Zum Anzeigen der Endzertifikate, (z. B. persönliche Zertifikate und die Zertifikate anderer Benutzer) drücken Sie die **Alt-Taste** und die **3**.

Zum Anzeigen persönlicher Zertifikate mit privaten Schlüsseln drücken Sie die **Alt-Taste** und die **9**.

Zum Anzeigen der Zertifikate anderer Benutzer drücken Sie die **Alt-Taste** und den **Punkt (.)**.

Zum Anzeigen der Stammzertifikate drücken Sie die **Alt-Taste** und die **1**.

Tastenkombinationen zum Anzeigen von Zertifikatinformationen

Zum Anzeigen des Zertifizierungsetiketts drücken Sie die **Leertaste**.

Zum Anzeigen der Zertifikatinformationen drücken Sie die **Eingabetaste**.

Zum Anzeigen der Sicherheitsstufe eines Zertifikats drücken Sie die **Alt-Taste** und gleichzeitig die Taste **L**.

Zum Anzeigen der Seriennummer für ein Zertifikat drücken Sie die **Alt-Taste** und gleichzeitig die Taste **8**.

Fehlerbehebung für Zertifikate

Das Herunterladen eines Zertifikats funktioniert nicht

Das Herunterladen eines Zertifikats funktioniert nicht

Wenn Sie den Verbindungstyp geändert haben, mit dem Ihr BlackBerry®-Gerät sich mit dem LDAP-Zertifikatsserver verbindet, versuchen Sie es mit dem Standardverbindungstyp neu.

Zertifikatserver

Info über Zertifikatserver

Hinzufügen eines Zertifikatsservers

Optionen für LDAP-Zertifikatserver

Optionen für OCSP- oder CRL-Zertifikatserver

Ändern von Zertifikatserverinformationen

Löschen eines Zertifikatsservers

Senden von Zertifikatserverinformationen an einen Ansprechpartner

Info über Zertifikatserver

Ihr BlackBerry®-Gerät arbeitet zum Suchen und Herunterladen von Zertifikaten mit einem Lightweight Directory Access Protocol (LDAP).

Zum Überprüfen des Zertifikatsperrstatus eines Zertifikats nutzt Ihr Gerät bei Bedarf Online Certificate Status Protocol (OCSP)-Server.

Zum Überprüfen des aktuell veröffentlichten Zertifikatsperrstatus eines Zertifikats nutzt Ihr Gerät CRL-Server (Certificate Revocation List). Auf CRL-Servern werden von Zertifizierungsstellen (Certificate authorities, CAs) Zertifikatsperrlisten veröffentlicht.

Verwandte Themen

Hinzufügen eines Zertifikatsservers (Siehe Seite 17.)

Hinzufügen eines Zertifikatsservers

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikatserver**.
3. Drücken Sie die **Menütaste**.

4. Klicken Sie auf **Neuer Server**.

5. Legen Sie das Feld **Servertyp** fest.

6. Geben Sie die entsprechenden Informationen für den Server ein.

7. Drücken Sie die **Menütaste**.

8. Klicken Sie auf **Speichern**.

Verwandte Themen

Optionen für LDAP-Zertifikatserver (Siehe Seite 17.)

Optionen für OCSP- oder CRL-Zertifikatserver (Siehe Seite 18.)

Optionen für LDAP-Zertifikatserver

- **Anzeigename:** Geben Sie den mit dem Server verbundenen gebräuchlichen Namen ein.
- **Servername:** Geben Sie die Netzwerkadresse des Servers ein.
- **Basisabfrage:** Geben Sie Informationen zur Basisabfrage ein, wie in Ihrem LDAP-Server konfiguriert. Der Inhalt erscheint in DN-Syntax (Distinguished Name) des X.509-Standards (z. B. o=test.rim.net).
- **Port:** Geben Sie die Portnummer ein, wie im Netzwerk Ihrer Organisation konfiguriert. Die Standard-Portnummer ist 389.
- **Authentifizierungstyp:** Gibt an, ob Sie zur Verbindung mit dem Server Authentifizierungsdaten benötigen.
- **Verbindungstyp:** Gibt an, ob die Verbindung zwischen dem BlackBerry®-Gerät und dem Server über SSL (Secure Sockets Layer) oder über TLS (Transport Layer Security) erfolgt.

Verwandte Themen

Hinzufügen eines Zertifikatsservers (Siehe Seite 17.)

Optionen für OCSP- oder CRL-Zertifikatserver

- **Anzeigename:** Geben Sie einen Namen für den Server ein.
- **Server-URL:** Geben Sie die Webadresse des Servers ein.

Verwandte Themen

Hinzufügen eines Zertifikatsservers (Siehe Seite 17.)

Ändern von Zertifikatserverinformationen

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikatserver**.
3. Markieren Sie einen Server.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Bearbeiten**.
6. Ändern Sie die entsprechenden Felder.
7. Drücken Sie die **Menütaste**.
8. Klicken Sie auf **Speichern**.

Verwandte Themen

Optionen für LDAP-Zertifikatserver (Siehe Seite 17.)

Optionen für OCSP- oder CRL-Zertifikatserver (Siehe Seite 18.)

Löschen eines Zertifikatsservers

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikatserver**.
3. Markieren Sie einen Server.

4. Drücken Sie die **Menütaste**.

5. Klicken Sie auf **Löschen**.

6. Klicken Sie auf **Ja**.

Verwandte Themen

Ändern von Zertifikatserverinformationen (Siehe Seite 18.)

Senden von Zertifikatserverinformationen an einen Ansprechpartner

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Zertifikatserver**.
3. Markieren Sie einen Server.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **E-Mail-Server** oder **PIN-Server**.

Verwandte Themen

Senden eines Zertifikats an einen Ansprechpartner (Siehe Seite 11.)

Anfügen eines Zertifikats an eine Nachricht (Siehe Seite 24.)

S/MIME-Nachrichten

Info über digitale Signaturen und Verschlüsselung

Info über Verschlüsselungssymbole

Info über Signatursymbole

Info über Nachrichtenklassifizierungen

Anzeigen des Zertifikats, mit dem eine Nachricht verschlüsselt wird

Anzeigen von Informationen über schwach verschlüsselte Nachrichten

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette

Herunterladen des Zertifikats eines Absenders

Importieren eines Zertifikats aus einer Nachricht

Importieren eines Zertifikats aus einer Anlage

Importieren von Zertifikats-serverinformationen aus einer Nachricht

Weiterleiten oder Beantworten einer S/MIME-Nachricht

Eine E-Mail-Nachricht digital signieren oder verschlüsseln

Eine PIN-Nachricht digital signieren oder verschlüsseln

Verschicken einer S/MIME-Nachricht mit einem anderen Zertifikat

Verschicken einer S/MIME-Nachricht ohne Zertifikat

Schützen einer S/MIME-Nachricht im Ordner mit gesendeten Elementen

Anzeigen einer Anlage in einer signierten Nachricht

Durchsuchen der Nachrichtenliste

Anfügen eines Zertifikats an eine Nachricht

Anzeigen kleiner Statussymbole für S/MIME-Nachrichten

Auswählen Ihres Standard-Signaturzertifikats für S/MIME

Auswählen Ihres Standard-S/MIME-Verschlüsselungszertifikats

Auswählen von Verschlüsselungs-algorithmen für S/MIME-Nachrichten

Anfordern signierter Bestätigungen für S/MIME-Nachrichten

Festlegen der Standard-Sicherheitsoptionen, mit denen Sie Nachrichten senden

Festlegen der Standard-Nachrichtenklassifikation, mit der Sie Nachrichten senden

Deaktivieren der Warnmeldung bei Verwendung eines nicht empfohlenen S/MIME-Zertifikats

Deaktivieren der Eingabe-aufforderung, die vor dem Abschneiden einer Nachricht angezeigt wird

Fehlerbehebung bei S/MIME-Nachrichten

Info über digitale Signaturen und Verschlüsselung

Sie können eine Nachricht digital signieren, damit der Empfänger die Authentizität und Integrität der Nachricht verifizieren kann. Wenn Sie mit Ihrem privaten Schlüssel eine Nachricht digital signieren, verifiziert der Empfänger mit Ihrem öffentlichen Schlüssel, ob die Nachricht wirklich von Ihnen und nicht von einer anderen Person gesendet wurde und ob niemand die Nachricht vor dem Empfang verändert hat.

Sie können eine Nachricht verschlüsseln, wenn Sie sie vertraulich behandelt wissen wollen. Zum Verschlüsseln Ihrer Nachricht verwendet Ihr BlackBerry®-Gerät den öffentlichen Schlüssel des Empfängers. Nur der private Schlüssel des Empfängers kann die Nachricht entschlüsseln und der Empfänger weiß, dass außer ihm niemand die Nachricht lesen kann.

Verwandte Themen

[Info über Verschlüsselungssymbole \(Siehe Seite 20.\)](#)

[Info über Signatursymbole \(Siehe Seite 20.\)](#)

Info über Verschlüsselungssymbole

Beim Öffnen einer verschlüsselten Nachricht zeigt ein Sperrsymbol den Verschlüsselungsstatus an. Ihr Systemadministrator richtet eine IT-Richtlinie ein, die bestimmt, ob der Verschlüsselungsalgorithmus der Nachricht als stark oder schwach eingestuft wird.

- **Sperrsymbol:** Die Nachricht ist stark verschlüsselt.
- **Sperrsymbol mit Fragezeichen:** Die Nachricht ist schwach verschlüsselt.

Verwandte Themen

[Info über Signatursymbole \(Siehe Seite 20.\)](#)

Info über Signatursymbole

Beim Öffnen einer digital signierten Nachricht zeigt ein Bandsymbol den Verifizierungsstatus der digitalen Signatur an.

- **Band mit Häkchen:** Ihr BlackBerry®-Gerät hat die digitale Signatur verifiziert.
- **Band mit X:** Ihr Gerät konnte die digitale Signatur nicht verifizieren.
- **Band mit Fragezeichen:** Ihr Gerät benötigt weitere Daten, um die digitale Signatur zu verifizieren.

Das Symbol nach dem Bandsymbol gibt den Status der Zertifikatskette des Absenderzertifikats an.

- **Zertifikat mit Häkchen:** Die Zertifikatskette ist vertrauenswürdig.
- **X:** Das Zertifikat des Absenders kann auf Ihrem Gerät nicht gefunden werden, ist gesperrt, nicht vertrauenswürdig oder kann nicht verifiziert werden, oder die E-Mail-Adresse des Absenders entspricht nicht der E-Mail-Adresse des Zertifikatempfängers im Zertifikat.
- **Fragezeichen:** Ihr Gerät benötigt weitere Daten, um den Vertrauensstatus zu verifizieren, das Zertifikat ist schwach, oder der Zertifikatsstatus ist nicht mehr aktuell.
- **Uhr:** Das Zertifikat des Absenders ist abgelaufen.

Verwandte Themen

[Info über Verschlüsselungssymbole \(Siehe Seite 20.\)](#)

Info über Nachrichtenklassifizierungen

Wurde auf Ihrem BlackBerry®-Gerät ein Konto eingerichtet, das BlackBerry Enterprise Server Version 4.1.2 oder höher verwendet, und hat Ihr Systemadministrator die Nachrichtenklassifizierung aktiviert, wendet der BlackBerry-Enterprise-Server auf jede Nachricht, die Sie erstellen, weiterleiten oder beantworten, eine Mindeststufe mit Sicherheitsaktionen an. Dies erfolgt entsprechend der Klassifizierung, die Sie der Nachricht geben. Ihr Systemadministrator konfiguriert die verschiedenen Nachrichtenklassifikationen, die Sie verwenden können.

Erhalten Sie eine Nachricht mit Nachrichtenklassifikation, erscheint die abgekürzte Klassifikation in der Betreffzeile der Nachricht und die vollständige Beschreibung der Klassifikation im Nachrichtenkörper. Die Abkürzung für die Klassifikation und die Beschreibung erscheinen ebenfalls in den Nachrichten in ihrem Ordner „Gesendete Objekte“.

Verwandte Themen

[Eine E-Mail-Nachricht digital signieren oder verschlüsseln \(Siehe Seite 22.\)](#)

Anzeigen des Zertifikats, mit dem eine Nachricht verschlüsselt wird

1. Öffnen Sie eine S/MIME-Nachricht, und markieren Sie das Verschlüsselungssymbol.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf die **Option zum Anzeigen des Verschlüsselungszertifikats**.

Verwandte Themen

Anzeigen von Zertifikatinformationen (Siehe Seite 9.)

Anzeigen von Informationen über schwach verschlüsselte Nachrichten

1. Öffnen Sie eine S/MIME-Nachricht, und markieren Sie das Verschlüsselungssymbol.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf **Verschlüsselungs-Details**.

Hinweis:

BlackBerry® Enterprise Server verschlüsselt in manchen Fällen Nachrichten neu, die mit einem schwachen Verschlüsselungsalgorithmus oder nur mit einer digitalen Signatur verschickt wurden.

Verwandte Themen

Info über Verschlüsselungssymbole (Siehe Seite 20.)

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette

1. Markieren Sie in einer geöffneten S/MIME-Nachricht die digitale Signatur oder das Symbol für den Vertrauensstatus.
2. Drücken Sie die **Menütaste**.
3. Führen Sie eine der folgenden Aktionen aus:
 - Um den Status des Absenderzertifikats zu prüfen, klicken Sie auf **Absenderzertifikat prüfen**.

- Um den Status des Absenderzertifikats und aller Zertifikate der Kette zu überprüfen, klicken Sie auf **Absenderzertifikatskette prüfen**.

Hinweis:

Die Menüeinträge „Absenderzertifikat prüfen“ und „Absenderzertifikatskette prüfen“ werden nur dann angezeigt, wenn das Zertifikat des Absenders in der Nachricht oder im Schlüsselspeicher Ihres BlackBerry®-Geräts enthalten ist.

Verwandte Themen

Überprüfen des Status eines Zertifikats oder einer Zertifikatskette (Siehe Seite 10.)

Herunterladen des Zertifikats eines Absenders

1. Markieren Sie in einer geöffneten S/MIME-Nachricht die digitale Signatur oder das Symbol für den Vertrauensstatus.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf **Absenderzertifikat abrufen**.

Hinweis:

Das Menüelement „Absenderzertifikat abrufen“ wird nur dann angezeigt, wenn das Zertifikat des Absenders nicht im Schlüsselspeicher Ihres BlackBerry®-Geräts oder in der Nachricht des Absenders enthalten ist.

Verwandte Themen

Herunterladen eines Zertifikats (Siehe Seite 8.)

Importieren eines Zertifikats aus einer Nachricht

1. Markieren Sie in einer geöffneten S/MIME-Nachricht die digitale Signatur oder das Symbol für den Vertrauensstatus.
2. Drücken Sie die **Menütaste**.

3. Klicken Sie auf **Absenderzertifikat importieren**.
4. Geben Sie Ihr Kennwort für den Schlüsselspeicher ein.
5. Klicken Sie auf **OK**.
6. Geben Sie ein Zertifizierungsetikett ein.
7. Klicken Sie auf **OK**.

Verwandte Themen

Herunterladen des Zertifikats eines Absenders (Siehe Seite 21.)

Herunterladen eines Zertifikats (Siehe Seite 8.)

Importieren eines Zertifikats aus einer Anlage

1. Klicken Sie in einer geöffneten Nachricht auf das Symbol für eine Zertifikatanlage.
2. Klicken Sie auf die **Schaltfläche zum Abrufen der Zertifikatanlage**.
3. Klicken Sie auf das Zertifikat.
4. Klicken Sie auf **Zertifikat importieren**.

Verwandte Themen

Herunterladen des Zertifikats eines Absenders (Siehe Seite 21.)

Herunterladen eines Zertifikats (Siehe Seite 8.)

Importieren von Zertifikats-serverinformationen aus einer Nachricht

1. Markieren Sie in einer geöffneten S/MIME-Nachricht das Symbol für einen S/MIME-Server.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf **Server importieren**.

Verwandte Themen

Hinzufügen eines Zertifikatservers (Siehe Seite 17.)

Weiterleiten oder Beantworten einer S/MIME-Nachricht

1. Klicken Sie in einer geöffneten Nachricht mit dem Trackball.
2. Klicken Sie auf **Weiterleiten** oder **Antworten**.

Verwandte Themen

Eine E-Mail-Nachricht digital signieren oder verschlüsseln (Siehe Seite 22.)

Ich kann nicht alle Optionen zum Signieren oder zur Verschlüsselung sehen (Siehe Seite 27.)

Eine E-Mail-Nachricht digital signieren oder verschlüsseln

1. Führen Sie in einer noch nicht gesendeten Nachricht eine der folgenden Aktionen durch:
 - Zum Anhängen einer digitalen Signatur wählen Sie im Feld **Codierung** die Option **Signieren**.
 - Zur Verschlüsselung der Nachricht wählen Sie im Feld **Codierung** die Option **Verschlüsseln**.
 - Zum Anhängen einer digitalen Signatur und zur Verschlüsselung der Nachricht wählen Sie im Feld **Codierung** die Option **Signieren und Verschlüsseln**.
2. Falls erforderlich, legen Sie die Einstellung für das Feld **Klassifizierung** fest.

Verwandte Themen

Auswählen Ihres Standard-Signaturzertifikats für S/MIME (Siehe Seite 25.)

Auswählen Ihres Standard-S/MIME-Verschlüsselungszertifikats (Siehe Seite 25.)

Auswählen von Verschlüsselungs-algorithmen für S/MIME-Nachrichten (Siehe Seite 25.)

Ich kann nicht alle Optionen zum Signieren oder zur Verschlüsselung sehen (Siehe Seite 27.)

Eine PIN-Nachricht digital signieren oder verschlüsseln

Führen Sie in einer noch nicht gesendeten Nachricht eine der folgenden Aktionen durch:

- Zum Anhängen einer digitalen Signatur wählen Sie im Feld **Codierung** die Option **Signieren**.
- Zur Verschlüsselung der Nachricht wählen Sie im Feld **Codierung** die Option **Verschlüsseln**.
- Zum Anhängen einer digitalen Signatur und zur Verschlüsselung der Nachricht wählen Sie im Feld **Codierung** die Option **Signieren und Verschlüsseln**.

Hinweis:

Zum Senden einer verschlüsselten PIN-Nachricht muss der Empfänger mit einer zugehörigen PIN-Nummer (Personal Identification Number) und E-Mail-Adresse in Ihrer Ansprechpartnerliste stehen. Ihr BlackBerry®-Gerät verwendet die E-Mail-Adresse aus Ihrer Ansprechpartnerliste, um ein Zertifikat für den Empfänger zu finden.

Verwandte Themen

Auswählen Ihres Standard-Signaturzertifikats für S/MIME (Siehe Seite 25.)

Auswählen Ihres Standard-S/MIME-Verschlüsselungszertifikats (Siehe Seite 25.)

Auswählen von Verschlüsselungs-algorithmen für S/MIME-Nachrichten (Siehe Seite 25.)

Ich kann nicht alle Optionen zum Signieren oder zur Verschlüsselung sehen (Siehe Seite 27.)

Verschicken einer S/MIME-Nachricht mit einem anderen Zertifikat

1. Legen Sie in einer nicht verschickten Nachricht für das Feld für die Verschlüsselung ein Zertifikat mit einer digitalen Signatur oder Verschlüsselung fest.
2. Drücken Sie die **Menütaste**.

3. Klicken Sie auf **Optionen**.
4. Wählen Sie ein anderes Zertifikat zum Signieren oder Verschlüsseln der Nachricht aus.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Speichern**.

Ihr BlackBerry®-Gerät verwendet das ausgewählte Zertifikat nur für die aktuelle Nachricht.

Verwandte Themen

Verschicken einer S/MIME-Nachricht ohne Zertifikat (Siehe Seite 23.)

Auswählen Ihres Standard-Signaturzertifikats für S/MIME (Siehe Seite 25.)

Auswählen Ihres Standard-S/MIME-Verschlüsselungszertifikats (Siehe Seite 25.)

Verschicken einer S/MIME-Nachricht ohne Zertifikat

1. Legen Sie in einer nicht verschickten Nachricht für das Feld für die Verschlüsselung ein Zertifikat mit einer digitalen Signatur fest.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf **Optionen**.
4. Setzen Sie das Feld **Zertifikat einfügen** in den Signaturoptionen auf **Nein**.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Speichern**.

Verwandte Themen

Verschicken einer S/MIME-Nachricht mit einem anderen Zertifikat (Siehe Seite 23.)

Schützen einer S/MIME-Nachricht im Ordner mit gesendeten Elementen

Wenn Sie eine Nachricht schützen, verschlüsselt Ihr BlackBerry®-Gerät die Nachricht beim Versenden nicht mit Ihrem, sondern mit dem Zertifikat des Empfängers. Geschützte Nachrichten können Sie auf Ihrem Gerät nicht lesen.

1. Setzen Sie in einer noch nicht gesendeten Nachricht das Feld **Codierung** auf eine Einstellung, die eine Verschlüsselung verwendet.
2. Drücken Sie die **Menütaste**.
3. Klicken Sie auf **Optionen**.
4. Legen Sie unter **Verschlüsselungsoptionen** für das Feld **Zertifikat** die Option für kein Zertifikat fest.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Speichern**.

Verwandte Themen

Eine E-Mail-Nachricht digital signieren oder verschlüsseln (Siehe Seite 22.)

Anzeigen einer Anlage in einer signierten Nachricht

Klicken Sie in einer geöffneten Nachricht auf die Anlage.

Verwandte Themen

Importieren eines Zertifikats aus einer Anlage (Siehe Seite 22.)

Durchsuchen der Nachrichtenliste

1. Drücken Sie in der Nachrichtenliste die **Menütaste**.
2. Klicken Sie auf **Suchen**.
3. Legen Sie die Suchkriterien fest.

4. Führen Sie eine der folgenden Aktionen aus:
 - Wenn Sie nur Nur-Text- und signierte Nachrichten durchsuchen möchten, setzen Sie die Einstellung im Feld **Einschließlich verschlüsselte Nachrichten** auf **Nein**.
 - Wenn Sie Nur-Text-, signierte und verschlüsselte Nachrichten durchsuchen möchten, setzen Sie die Einstellung im Feld **Einschließlich verschlüsselte Nachrichten** auf **Ja**.
5. Klicken Sie mit dem Trackball.
6. Klicken Sie auf **Suchen**.

Hinweis:

Wenn Sie die Einstellung im Feld „Einschließlich verschlüsselte Nachrichten“ auf „Ja“ gesetzt haben und die Sicherheitsstufe für den privaten Schlüssel auf mittel oder hoch eingestellt ist, werden Sie möglicherweise zur Eingabe Ihres Kennworts für den Schlüsselspeicher aufgefordert, bevor die Suchergebnisse angezeigt werden.

Verwandte Themen

Einstellen der Speicherdauer Ihres Schlüsselspeicher-Kennworts (Siehe Seite 24.)

Anfügen eines Zertifikats an eine Nachricht

1. Drücken Sie in einer noch nicht gesendeten Nachricht die **Menütaste**.
2. Klicken Sie auf **Zertifikate anfügen**.
3. Markieren Sie ein Zertifikat.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Fortfahren**.

Verwandte Themen

Senden eines Zertifikats an einen Ansprechpartner (Siehe Seite 11.)

Anzeigen kleiner Statussymbole für S/MIME-Nachrichten

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Legen Sie im Feld **Nachrichtenanzeige-Symbole** die Option **Klein** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Info über Verschlüsselungssymbole (Siehe Seite 20.)

Info über Signatursymbole (Siehe Seite 20.)

Auswählen Ihres Standard-Signaturzertifikats für S/MIME

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Legen Sie in den Signaturoptionen eine Einstellung für das Feld **Zertifikat** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Verschicken einer S/MIME-Nachricht mit einem anderen Zertifikat (Siehe Seite 23.)

Auswählen Ihres Standard-S/MIME-Verschlüsselungszertifikats

Ihr BlackBerry®-Gerät verschlüsselt die Nachrichten im Ordner der gesendeten Elemente mit dem festgelegten Zertifikat und fügt dieses in S/MIME-Nachrichten (Secure Multipurpose Internet Mail Extensions) ein, so dass die Empfänger dieser Nachrichten ihre Antworten verschlüsseln können.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Legen Sie unter **Verschlüsselungsoptionen** eine Einstellung für das Feld **Zertifikat** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Verschicken einer S/MIME-Nachricht mit einem anderen Zertifikat (Siehe Seite 23.)

Auswählen von Verschlüsselungsalgorithmen für S/MIME-Nachrichten

Geht eine Nachricht an mehrere Empfänger, verwendet Ihr BlackBerry®-Gerät den ersten ausgewählten Inhalts-Chiffrierschlüssel, den bekanntermaßen alle Empfänger unterstützen.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Wählen Sie alle Inhalts-Chiffrierschlüssel aus, die Ihnen zur Verschlüsselung von Nachrichten zur Verfügung stehen sollen.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Eine E-Mail-Nachricht digital signieren oder verschlüsseln (Siehe Seite 22.)

Anfordern signierter Bestätigungen für S/MIME-Nachrichten

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.

3. Setzen Sie das Feld zum Anfordern der S/MIME-Bestätigung auf **Ja**.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Eine E-Mail-Nachricht digital signieren oder verschlüsseln (Siehe Seite 22.)

Festlegen der Standard-Sicherheitsoptionen, mit denen Sie Nachrichten senden

Ihr BlackBerry®-Gerät verwendet die Standard-Codierung für Kontakte, denen Sie noch keine Nachricht gesendet haben.

1. Klicken Sie in den Geräteoptionen auf **Erweiterte Optionen**.
2. Klicken Sie auf **Nachrichtendienste**.
3. Legen Sie die Einstellung für das Feld **Standard-Codierung** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Einstellen der Speicherdauer Ihres Schlüsselspeicher-Kennworts (Siehe Seite 24.)

Festlegen der Standard-Nachrichtenklassifikation, mit der Sie Nachrichten senden

Vergewissern Sie sich, dass Ihr Systemadministrator Nachrichtenklassifizierungen eingerichtet hat.

Ihr BlackBerry®-Gerät verwendet die Standard-Nachrichtenklassifizierung für Kontakte, denen Sie noch keine Nachricht gesendet haben.

1. Klicken Sie in den Geräteoptionen auf **Erweiterte Optionen**.

2. Klicken Sie auf **Nachrichtendienste**.
3. Legen Sie die Einstellung für das Feld **Standardklassifizierung** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Info über Nachrichtenklassifizierungen (Siehe Seite 20.)

Deaktivieren der Warnmeldung bei Verwendung eines nicht empfohlenen S/MIME-Zertifikats

Standardmäßig wird eine Meldung angezeigt, wenn Sie beim Versenden einer Nachricht ein Zertifikat verwenden, dessen Einsatz nicht empfohlen wird, z. B. ein schwaches oder ein abgelaufenes Zertifikat.

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Setzen Sie die **Warnung für problematische Zertifikate** auf **Nein**.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Möchten Sie wieder eine Warnmeldung erhalten, setzen Sie die **Warnung für problematische Zertifikate** wieder auf **Ja**.

Deaktivieren der Eingabeaufforderung, die vor dem Abschneiden einer Nachricht angezeigt wird

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.

3. Legen Sie im Feld für die **Warnung bei abgeschnittenen Nachrichten** die Option **Nein** fest.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Wenn Sie wieder eine Warnmeldung erhalten möchten, legen Sie im Feld für die Warnung bei abgeschnittenen Nachrichten die Option **Ja** fest.

Fehlerbehebung bei S/MIME-Nachrichten

Ich kann nicht alle Optionen zum Signieren oder zur Verschlüsselung sehen

Ich kann nicht alle Optionen zum Signieren oder zur Verschlüsselung sehen

Führen Sie eine der folgenden Aktionen aus:

- Überprüfen Sie, ob die aktuell ausgewählte Nachrichtenklassifikation die gewünschten Signatur- oder Verschlüsselungsoptionen unterstützt. Versuchen Sie es mit einer anderen Nachrichtenklassifikation.
- Vergewissern Sie sich, dass Ihr Nachrichtendienst so konfiguriert ist, dass alle Signatur- und Verschlüsselungsoptionen unterstützt werden.

Verwandte Themen

Info über Nachrichtenklassifizierungen (Siehe Seite 20.)

Smart Cards

Info über Smartcards

Voraussetzungen für die Zwei-Faktor-Authentifizierung

Aktivieren der Zwei-Faktor-Authentifizierung

Entsperren Ihres BlackBerry-Geräts bei aktivierter Zwei-Faktor-Authentifizierung

Verbinden Ihres BlackBerry-Geräts mit dem BlackBerry Smart Card Reader

Importieren eines Zertifikats von einer Smartcard

Einstellen der Zeitdauer ohne eine Verbindung, nach der der BlackBerry Smart Card Reader ausgeschaltet wird

Einstellen der Aktivitätsstufe des BlackBerry Smart Card Reader

Einrichten des Bluetooth-Bereichs für den BlackBerry Smart Card Reader

Einstellen der Bluetooth-Verbindungstrennung

Einstellen von Optionen zum Löschen der sicheren Kopplungs-informationen für den BlackBerry Smart Card Reader

Info über Smartcards

Zertifikate und private Schlüssel werden auf Smartcards gespeichert. Sie können Zertifikate in den Schlüsselspeicher Ihres BlackBerry®-Geräts importieren, private Schlüssel aber nur auf Smartcards speichern. Aus diesem Grund wird bei Bearbeitungen mit privaten Schlüsseln, z. B. dem Signieren und der Entschlüsselung, die Smartcard eingesetzt. Bearbeitungen mit öffentlichen Schlüsseln, z. B. das Verifizieren und die Verschlüsselung werden auf Ihrem Gerät ausgeführt.

Mit Hilfe eines Smart Card Readers können Sie Zertifikate von einer Smartcard auf Ihr Gerät laden, Sie können ein Smartcard-Zertifikat zur Authentifizierung mit Ihrem Gerät verwenden sowie S/MIME-(Secure Multipurpose Internet Mail Extensions-)Nachrichten mit Ihren Smartcard-Zertifikaten schicken.

Wenn Sie ein Smartcard-Zertifikat zur Authentifizierung mit Ihrem Gerät benutzen, schickt Ihr Gerät, nachdem Sie den Smart Card Reader mit Ihrem Gerät verbinden, immer wenn Sie Ihr Gerät entsperren, eine Authentifizierungsanforderung an die Smartcard.

Verwandte Themen

Importieren eines Zertifikats von einer Smartcard (Siehe Seite 30.)

Aktivieren der Zwei-Faktor-Authentifizierung (Siehe Seite 30.)

Voraussetzungen für die Zwei-Faktor-Authentifizierung

- Vergewissern Sie sich, dass Sie ein Kennwort für das BlackBerry®-Gerät eingerichtet haben.
- Vergewissern Sie sich, dass Sie das Smart-Card-Kennwort kennen. In der Regel wird das Kennwort mit der Smartcard mitgeliefert.

Verwandte Themen

Aktivieren der Zwei-Faktor-Authentifizierung (Siehe Seite 30.)

Aktivieren der Zwei-Faktor-Authentifizierung

1. Klicken Sie in den Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Allgemeine Einstellungen**.
3. Stellen Sie das Feld **Benutzerauthentifizierer** auf **Aktiviert** ein.
4. Drücken Sie die **Menütaste**.
5. Klicken Sie auf **Speichern**.

Verwandte Themen

Voraussetzungen für die Zwei-Faktor-Authentifizierung (Siehe Seite 29.)

Entsperren Ihres BlackBerry-Geräts bei aktivierter Zwei-Faktor-Authentifizierung (Siehe Seite 30.)

Einrichten des Bluetooth-Bereichs für den BlackBerry Smart Card Reader (Siehe Seite 31.)

Entsperren Ihres BlackBerry-Geräts bei aktivierter Zwei-Faktor-Authentifizierung

Vergewissern Sie sich, dass Sie das Smart-Card-Kennwort kennen. In der Regel wird das Kennwort mit der Smartcard mitgeliefert.

1. Klicken Sie auf Ihrem BlackBerry®-Gerät auf dem Bildschirm mit der Sicherheitssperre mit dem Trackball.
2. Klicken Sie auf **Entsperren**.
3. Geben Sie Ihr BlackBerry-GeräteKennwort ein.
4. Drücken Sie die **Eingabetaste**.
5. Geben Sie das Authentifizierungskennwort für die Smartcard ein.
6. Drücken Sie die **Eingabetaste**.

Verwandte Themen

Aktivieren der Zwei-Faktor-Authentifizierung (Siehe Seite 30.)

Verbinden Ihres BlackBerry-Geräts mit dem BlackBerry Smart Card Reader

1. Klicken Sie in den BlackBerry®-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.
5. Drücken Sie die **Menütaste**.
6. Klicken Sie auf **Verbinden**.

Drücken Sie die **Menütaste**, um das BlackBerry-Gerät vom BlackBerry Smart Card Reader zu trennen. Klicken Sie auf **Verbindung trennen**.

Verwandte Themen

Einstellen der Zeitdauer ohne eine Verbindung, nach der der BlackBerry Smart Card Reader ausgeschaltet wird (Siehe Seite 31.)

Importieren eines Zertifikats von einer Smartcard

1. Klicken Sie in den BlackBerry®-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **S/MIME**.
3. Drücken Sie die **Menütaste**.
4. Klicken Sie auf **Smartcard-Zertifikate importieren**.
5. Wählen Sie ein Zertifikat aus.
6. Klicken Sie auf **OK**.
7. Geben Sie Ihr Kennwort für den Schlüsselspeicher ein.
8. Klicken Sie auf **OK**.

Hinweis:

Um ein Zertifikat importieren zu können, benötigen Sie eine PKI-(Public Key Infrastructure-)Systemlizenz.

Verwandte Themen

Info über Smartcards (Siehe Seite 29.)

Einstellen der Zeitdauer ohne eine Verbindung, nach der der BlackBerry Smart Card Reader ausgeschaltet wird

Vergewissern Sie sich, dass Ihr BlackBerry®-Gerät mit dem BlackBerry Smart Card Reader verbunden ist.

Sie können im Feld „Timeout bei Ausschalten des Geräts“ eine kürzere Zeitdauer einstellen, um den Akku zu schonen.

1. Klicken Sie in den BlackBerry-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.
5. Stellen Sie im Abschnitt **Einstellungen des Lesegeräts** das Feld **Timeout bei Ausschalten des Geräts** auf die Zeitdauer ein, die ohne eine Bluetooth®-Verbindung verstreichen soll, bevor sich der BlackBerry Smart Card Reader ausschaltet.
6. Drücken Sie die **Menütaste**.
7. Klicken Sie auf **Speichern**.

Verwandte Themen

Einstellen der Bluetooth-Verbindungstrennung (Siehe Seite 32.)

Einstellen der Aktivitätsstufe des BlackBerry Smart Card Reader

Vergewissern Sie sich, dass Ihr BlackBerry®-Gerät mit dem BlackBerry Smart Card Reader verbunden ist.

Das Einstellen des BlackBerry Smart Card Reader auf eine höhere Aktivitätsstufe trägt zur Verbesserung der Leistung bei, beansprucht den Akku jedoch mehr als niedrige Aktivitätsstufen.

1. Klicken Sie in den BlackBerry-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.
5. Führen Sie im Abschnitt **Einstellungen des Lesegeräts** eine der folgenden Aktionen durch:
 - Um den BlackBerry Smart Card Reader auf die niedrigste Aktivitätsstufe einzustellen, damit er nur dann aktiv ist, wenn Smartcard-Aktionen, z. B. Importieren von Zertifikaten, Signieren von E-Mail-Nachrichten oder Entschlüsseln von E-Mail-Nachrichten, ausgeführt werden, stellen Sie das Feld **Batteriesparmodus** auf **Voll** ein.
 - Um den BlackBerry Smart Card Reader auf eine mittlere Aktivitätsstufe einzustellen, so dass er nur dann aktiv ist, wenn die BlackBerry-Geräte bzw. Computer, mit denen er verbunden ist, nicht gesperrt sind, wählen Sie **Teilweise**.
 - Um den BlackBerry Smart Card Reader auf die höchste Aktivitätsstufe einzustellen, so dass er immer aktiv ist, wählen Sie **Deaktiviert**.
6. Drücken Sie die **Menütaste**.
7. Klicken Sie auf **Speichern**.

Einrichten des Bluetooth-Bereichs für den BlackBerry Smart Card Reader

Vergewissern Sie sich, dass Ihr BlackBerry®-Gerät mit dem BlackBerry Smart Card Reader verbunden ist.

Bei einer Zwei-Faktor-Authentifizierung empfiehlt es sich, die Bluetooth®-Technologie auf dem BlackBerry Smart Card Reader auf eine kürzere Distanz einzustellen, um sicherzustellen, dass Ihr BlackBerry-Gerät schnell gesperrt wird, wenn sich der BlackBerry Smart Card Reader nicht in Reichweite befindet. Wenn Sie Änderungen im Feld „Bluetooth-Bereich“ vornehmen, wird die Bluetooth-Verbindung getrennt, und Sie müssen Ihr BlackBerry-Gerät erneut mit Ihrem BlackBerry Smart Card Reader verbinden.

1. Klicken Sie in den BlackBerry-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.
5. Stellen Sie im Abschnitt **Einstellungen des Lesegeräts** das Feld **Bluetooth-Bereich** auf die gewünschte Distanz für die Bluetooth-Technologie auf dem BlackBerry Smart Card Reader ein. Um für die Bluetooth-Technologie zum Beispiel die kürzeste Distanz zu wählen, stellen Sie das Feld **Bluetooth-Bereich** auf **30 %** ein.
6. Drücken Sie die **Menütaste**.
7. Klicken Sie auf **Speichern**.

Hinweis:

Der physische Bereich für die Bluetooth-Technologie auf dem BlackBerry Smart Card Reader kann sich je nach der Umgebung, in der der BlackBerry Smart Card Reader verwendet wird, ändern.

Verwandte Themen

[Einstellen der Bluetooth-Verbindungstrennung](#) (Siehe Seite 32.)

Einstellen der Bluetooth-Verbindungstrennung

In jedem Zeitraum sendet Ihr BlackBerry®-Gerät ein Signal (Heartbeat) aus, das vom BlackBerry Smart Card Reader erkannt wird. Wenn Ihr BlackBerry-Gerät oder der BlackBerry Smart Card Reader das Heartbeat-Signal bzw. die Antwort nicht auffängt, wird die Bluetooth®-Verbindung getrennt.

1. Klicken Sie in den BlackBerry-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.
5. Stellen Sie im Abschnitt **Einstellungen des Lesegeräts** das Feld **Heartbeat-Zeit für Verbindung** ein.
6. Drücken Sie die **Menütaste**.
7. Klicken Sie auf **Speichern**.

Verwandte Themen

[Einrichten des Bluetooth-Bereichs für den BlackBerry Smart Card Reader](#) (Siehe Seite 31.)

Einstellen von Optionen zum Löschen der sicheren Kopplungs-informationen für den BlackBerry Smart Card Reader

1. Klicken Sie in den BlackBerry-Geräteoptionen auf **Sicherheitsoptionen**.
2. Klicken Sie auf **Smart Card**.
3. Klicken Sie im Abschnitt **Registrierte Reader-Treiber** auf **BlackBerry**.
4. Klicken Sie auf **Treibereinstellungen**.

5. Führen Sie im Abschnitt **Schlüssel löschen** nach eine oder mehrere der folgenden Aktionen durch:

- Stellen Sie im Feld **Timeout nach Verbindungsabbau** die Zeitdauer ein, die nach dem Trennen einer Bluetooth®-Verbindung verstreichen soll, bevor Ihr BlackBerry-Gerät und Ihr BlackBerry Smart Card Reader die Informationen über den sicheren Kopplungsschlüssel löschen.
- Geben Sie im Feld **ALLE Schlüssel löschen** ein, ob Ihr BlackBerry-Gerät die sicheren Kopplungsschlüssel für gekoppelte Computer löschen soll, wenn das Timeout nach dem Verbindungsabbau erfolgt.
- Stellen Sie im Feld **Langzeittimeout** die Zeitdauer ein, die verstreichen soll, bevor Ihr BlackBerry-Gerät und Ihr BlackBerry Smart Card Reader die Informationen über den sicheren Kopplungsschlüssel löschen.
- Stellen Sie im Feld **Timeout nach Inaktivität** die Zeitdauer ohne sicheren Bluetooth-Datenverkehr zwischen Ihrem BlackBerry-Gerät und Ihrem BlackBerry Smart Card Reader ein, die verstreichen soll, bevor das BlackBerry-Gerät und der BlackBerry Smart Card Reader die Informationen über sichere Kopplungen löschen.
- Stellen Sie im Feld **Timeout nach Entnahme der Smartcard** die Zeitdauer nach Entnahme der Smartcard aus Ihrem BlackBerry Smart Card Reader ein, die verstreichen soll, bevor Ihr BlackBerry-Gerät und Ihr BlackBerry Smart Card Reader die Informationen über sichere Kopplungen löschen.
- Geben Sie im Feld **Anzahl der Transaktionen** an, wie viele Transaktionen erfolgen sollen, bevor Ihr BlackBerry-Gerät und Ihr BlackBerry Smart Card Reader die Informationen über den sicheren Kopplungsschlüssel löschen.

6. Drücken Sie die Menütaste.

7. Klicken Sie auf **Speichern**.

Falls Ihr BlackBerry®-Gerät und Ihr BlackBerry Smart Card Reader die Informationen über sichere Kopplungen löschen, müssen Sie den BlackBerry Smart Card Reader neu verbinden, um auf die Smartcard zugreifen zu können.

Verwandte Themen

[Einrichten des Bluetooth-Bereichs für den BlackBerry Smart Card Reader \(Siehe Seite 31.\)](#)

[Einstellen der Bluetooth-Verbindungstrennung \(Siehe Seite 32.\)](#)

Rechtliche Hinweise

© 2007 Research In Motion Limited. Alle Rechte vorbehalten. Die Marken, Abbildungen und Symbole der BlackBerry- und RIM-Familie sind ausschließliches Eigentum von Research In Motion Limited. RIM, Research In Motion, BlackBerry, BlackBerry, „Always On, Always Connected“ und das „Envelope in Motion“-Symbol sind beim Patent and Trademark Office in den USA eingetragen und können in anderen Ländern ebenfalls eingetragen oder angemeldet sein.

Die Bluetooth®-Wortmarke und -Logos sind Eigentum von Bluetooth SIG, Inc. und jegliche Verwendung solcher Marken durch Research In Motion erfolgt unter Lizenz. Entrust, Entrust Entelligence und Entrust Authority sind entweder eingetragene Marken oder Marken von Entrust, Inc. in den USA und bestimmten anderen Ländern. Microsoft und Windows sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Alle weiteren Warenzeichen, Produkt- und Firmennamen, Marken und Dienstleistungsmarken sind Eigentum ihrer jeweiligen Inhaber.

Das BlackBerry-Gerät, der BlackBerry Smart Card Reader sowie die zugehörige Software sind durch Urheberrechtsgesetze und Bestimmungen internationaler Verträge sowie eines oder mehrere der folgenden Patente geschützt. Die US-Patentnummern lauten: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Weitere Patente sind angemeldet oder stehen zur Anmeldung in verschiedenen Ländern der Welt an. Eine aktuelle Liste der RIM-Patente (gemäß nachfolgender Definition) finden Sie unter www.rim.com/patents.

Alle Angaben in diesem Dokument sind ohne Gewähr. Research In Motion Limited und seine angegliederten Unternehmen („RIM“) übernehmen keine Verantwortung für eventuelle typographische, technische oder anderweitige Ungenauigkeiten in diesem Dokument. Dieses Dokument nennt eventuell einige Aspekte der RIM-Technologie im Allgemeinen, um das Eigentum und die vertraulichen Informationen von RIM und/oder Handelsgeheimnisse zu schützen. RIM behält sich das Recht vor, die in diesem Dokument enthaltenen Informationen von Zeit zu Zeit zu ändern. RIM ist jedoch nicht verpflichtet, den Benutzer von diesen Änderungen, Aktualisierungen, Verbesserungen oder Zusätzen rechtzeitig bzw. überhaupt in Kenntnis zu setzen. RIM ÜBERNIMMT KEINE REPRÄSENTANZEN, GEWÄHRLEISTUNGEN, BEDINGUNGEN ODER VERTRAGLICHE VERPFLICHTUNGEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN ODER BEDINGUNGEN BEZÜGLICH DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, NICHTVERLETZUNG, HANDELSTAUGLICHKEIT, WIDERSTANDSFÄHIGKEIT, TITEL ODER IN BEZUG AUF LEISTUNG ODER NICHT LEISTUNG JEDLICHER SOFTWARE, AUF DIE HIER BEZUG GENOMMEN WIRD, ODER DIE LEISTUNG BELIEBIGER DIENSTE, AUF DIE HIER BEZUG GENOMMEN WIRD). IN VERBINDUNG MIT IHRER NUTZUNG DIESER DOKUMENTATION HAFTET RIM SOWIE SEINE GESCHÄFTSFÜHRUNG, LEITENDEN ANGESTELLTEN, BESCHÄFTIGTEN ODER BERATER FÜR KEINE SCHÄDEN ODER FOLGESCHÄDEN, UNABHÄNGIG DAVON, OB DIESE DIREKTER, ÖKONOMISCHER, GEWERBLICHER, SPEZIELLER, ZUFÄLLIGER,

EXEMPLARISCHER ODER INDIREKTER NATUR SIND. DIES GILT AUCH, WENN RIM AUF DIE MÖGLICHKEIT VON SCHÄDEN HINGEWIESEN WURDE. DIES BETRIFFT OHNE EINSCHRÄNKUNG DEN VERLUST VON GESCHÄFTSEINKOMMEN, DATENVERLUST, DURCH VERZÖGERUNG ENTSTANDENE SCHÄDEN, ENTGANGENEN PROFIT ODER DAS AUSBLEIBEN ERWARTETER EINSPARUNGEN.

Dieses Dokument kann Verweise auf Informationsquellen, Hardware oder Software, Produkte oder Services und/oder Websites von Dritten enthalten (zusammenfassend „Informationen Dritter“ genannt). Weder steuert RIM beliebige Drittanbieter-Informationen noch ist RIM für diese Informationen verantwortlich, einschließlich, ohne Einschränkung, Inhalt, Genauigkeit, Einhaltung der Urheberrechtsgesetze, Leistung, Kompatibilität, Zuverlässigkeit, Rechtmäßigkeit, Anstand, Links oder jeder weitere Aspekt der Drittanbieter-Informationen. Das Vorhandensein von Drittanbieter-Informationen in diesem Dokument unterstellt keine Billigung seitens RIM dieser Drittanbieter-Informationen oder des Drittanbieters selbst. Die Installation und Nutzung von Drittanbieterinformationen in Verbindung mit den Produkten und Dienstleistungen von RIM setzen eventuell ein oder mehrere Patente, Warenzeichen oder Urheberrechtslizenzen voraus, um eine Verletzung der geistigen Eigentumsrechte von Dritten zu vermeiden. Jegliche Transaktionen mit Informationen Dritter, einschließlich und ohne Einschränkung der Einhaltung geltender Lizenzierungsanforderungen und Bedingungen und Bestimmungen, finden ausschließlich zwischen Ihnen und dem Dritten statt. Sie allein sind dafür verantwortlich zu prüfen, ob solche Drittlizenzen erforderlich sind, und Sie sind ebenfalls dafür zuständig, jegliche solche mit Informationen Dritter in Zusammenhang stehende Lizenzen zu erwerben. Soweit Lizenzen für geistiges Eigentum erforderlich sind, empfiehlt RIM ausdrücklich, dass Sie die Informationen Dritter erst dann installieren oder nutzen, wenn alle relevanten Lizenzen von Ihnen oder in Ihrem Namen erstanden wurden. Ihre Nutzung von

Drittanbieterinformationen erfolgt unter der Voraussetzung, dass Sie den Bedingungen der Lizenzen für Drittanbieterinformationen zustimmen. Die Bereitstellung von Drittanbieterinformationen, die zusammen mit den Produkten und Dienstleistungen von RIM angeboten werden, erfolgt ohne Mängelgewähr. RIM übernimmt keinerlei Verantwortung, Gewährleistung oder Garantie hinsichtlich der Drittanbieterinformationen sowie keinerlei Haftung in Bezug auf Drittanbieterinformationen, selbst dann nicht, wenn RIM von der Möglichkeit solcher Schäden in Kenntnis gesetzt wurde oder solche Schäden voraussehen kann.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Kanada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
Großbritannien

Veröffentlicht in Kanada