Defense Security Service
Office of the Designated Approval Authority
Process for Clearing a Blackberry

This process is recommended for use by Industry when a Blackberry must be cleared as a result of a security incident involving contamination of the unclassified device by receipt of emails classified as Secret or below. Contamination above Secret (i.e., Top Secret, Sensitive Compartmented Information (SCI), Special Access Programs (SAP), etc.) requires confiscation and destruction of the Blackberry.

Throughout the procedure, Industry will be responsible for the process as a whole, and will provide response to Government personnel as required. This document details the contractor's responsibility in the over-all cleanup process as it relates to the erasing of Blackberry devices. The government contracting agency (GCA) as the data owner may specify other methods or procedures to be used in lieu of this one.

Table of Contents

Table of Figures

9/6/2006

1.0   Introduction

Since the use of BlackBerry personal digital assistants (PDA) have become a normal part of the communication landscape, the problem of email contamination (i.e., classified information inadvertently placed on unclassified systems) has migrated to these devices. Procedures for cleaning up contaminations on email servers have been in existence for several years and the same thought processes should be applied to the clean up of spills on BlackBerrys.   The differences are that BlackBerry devices do not allow themselves to be overwritten in the same manner as a standard computer and they are of course mobile. Incorporating a well thought out risk management position with documented procedures will allow this technology to be used to full advantage and still provide insurance that contaminations are contained and addressed in an adequate manner.

Data remanence is residual information left on a medium after an erasure or deletion has occurred. When data on storage media is cleared or erased, there are often physical characteristics that allow data reconstruction. Contaminated BlackBerrys must be carefully managed due to the residual data remaining on the device and the unit's susceptibility to loss, theft, or duplication.

Currently, there is no known method other than destruction for completely assuring that residual classified information has been completely removed from a BlackBerry; also known as sanitization. Therefore, DSS recommends that all contaminated Blackberry devices be cleared of using RIM recommended procedures as outlined below and destroyed at end of life.

2.0   Administrative Requirements

Addressed in the user manual and other guidance documents are a number of methods for removing data from a BlackBerry. The following procedure in Section 3 is only one of those methods. Although described here in depth, it is not recommended over alternate methods provided without detailed instructions in Section 4.

The following procedures do not sanitize BlackBerrys and are not to be used for sanitizing the device for turn-in or release outside DoD or DoD Cleared Contractor control. These procedures are approved only for data spillage involving information classified as Secret and below. Top Secret, Secret Restricted Data, and SCI/SAP contaminations require the BlackBerry be confiscated and destroyed by the cognizant security official.

All contaminations and Blackberry devices cleared utilizing this procedure must be documented as required by NISPOM paragraphs 1-303 and 1-304. Also, the user responsible, serial number of the device, and dates of occurrence must be recorded and maintained for a minimum of two (2) years after the device is destroyed.

3.0   Description

3.1   Overview of BlackBerry Data Storage

BlackBerry devices utilize a type of data storage called flash memory. Flash memory is a solid-state, non-volatile, rewritable memory that functions like a combination of RAM and a hard disk. Flash memory stores bits of electronic data in memory cells, but also retains the data in memory when the power is turned off. Unlike some handheld devices, such as Palm Organizers, which use battery backed flash ram, BlackBerry flash memory is not dependent on battery life. Data stored in a Blackberry's flash memory can remain resident for years without a power source.

Another feature of flash memory is that data is written and erased in large blocks instead of individual bytes. Flash memory is organized so that a complete block of memory cells can be erased in a single action, or "flash". In addition, flash memory is optimized so that reads and writes to the medium are much faster than full erasures. Considering the challenges of processor and battery power in handheld units, it is extremely inefficient for the units to perform erasures. This concept of block erasures guarantees that the storage medium will have data remanence. As an example, the typical message size on a BlackBerry device is two kilobytes. In order for the device to erase the message, it would have to erase an entire block of 64 kilobytes, which most likely contains messages that have not yet been deleted. Instead, the message is marked as deleted in the Blackberry database and the system simply ignores the old data still present in the unit. Assuming the typical message data space on a BlackBerry unit is two megabytes, up to 1000 deleted emails could be resident in the unallocated space of the device.

3.2   Blackberry Clearing Processes

There are a number of ways to clear Blackberry devices that have become contaminated with classified information. The detailed instruction below is one way. Additional methods are included in section 4.

3.2.1   Blackberry Desktop Manager

The same version of the Blackberry or the desktop manager used in this document can be downloaded from the Research In Motion web site (http://www.rim.net/).
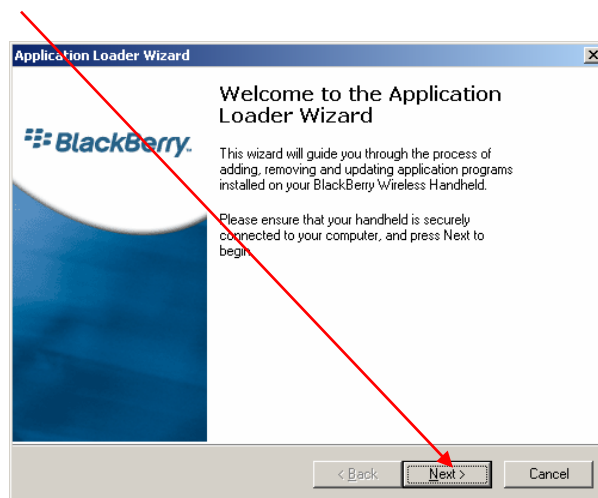
Open the **Blackberry Desktop Manager** and double click on the <**Application Loader**> as shown below in Figure 1.
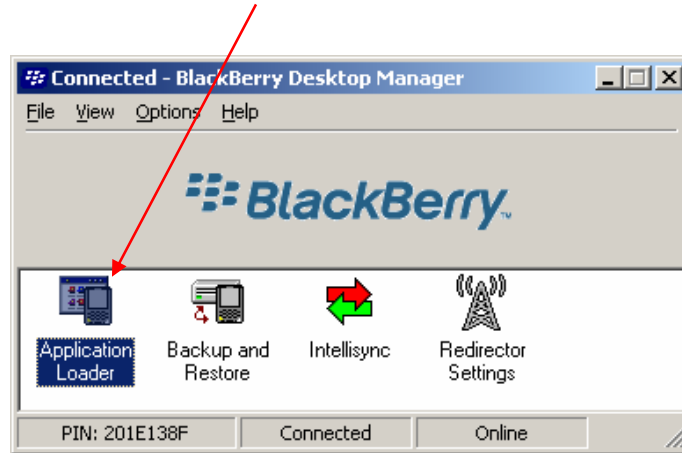
Figure 1. Blackberry Desktop Manager

3.2.2   Application Loader Startup

When the application loader is opened the following screen will appear. Click <**Next**> to continue.

Figure 2. Application Loader Startup

5

3.2.3 Application Loader Wizard – Selecting Options

The next screen will appear as shown below in Figure 3. Click <**Next>** to continue.
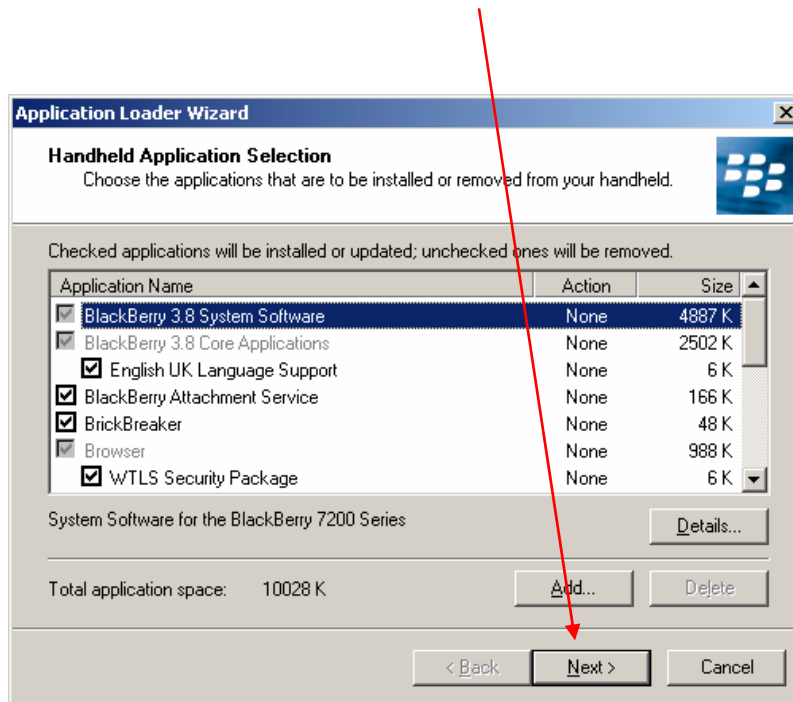

Figure 3. Selecting Options

Note: If the Blackberry is configured with a password, the user will be prompted at this point for that password. If no applications are loaded, it will be displayed on the screen and the only options available will be the Add or Cancel buttons. The user will not be able to get to the next screen (Figure 4).

Completing Application Loader

Since all necessary applications should have been installed when the Blackberry was initailly setup, the application loader will state that **No actions are required** as shown below in Figure 4.
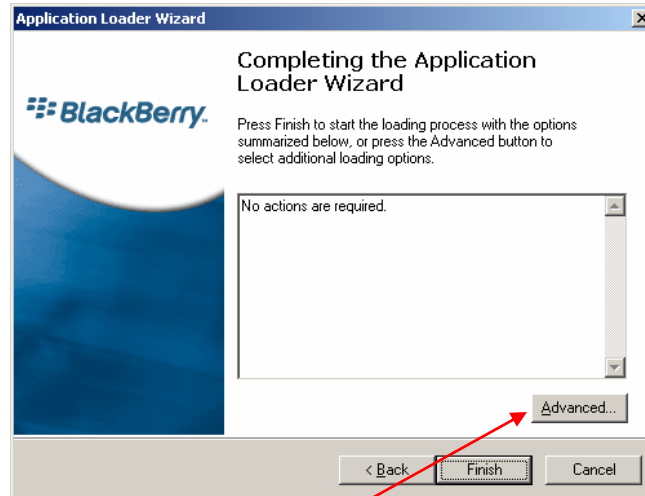

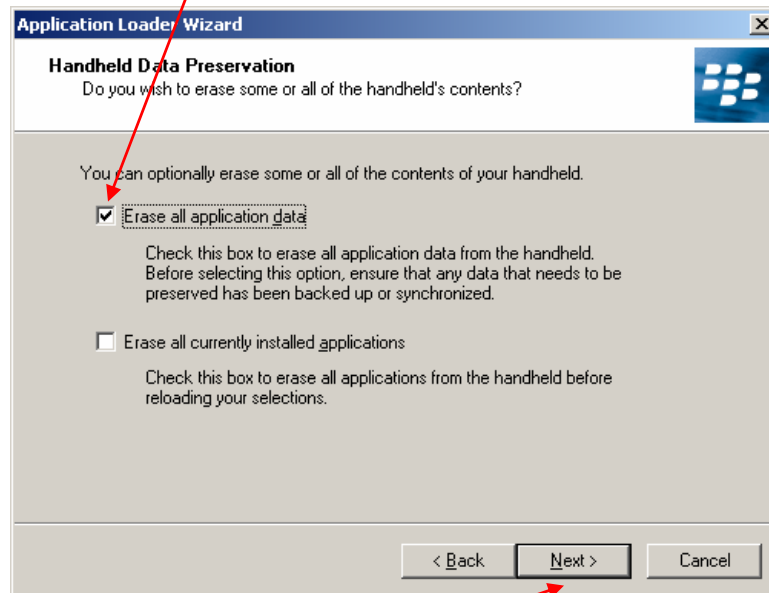**Figure 4. Completing Application Loader**

Please click <**Advanced>** to proceed.

3.2.4 Handheld Data Preservation

The next screen will be the Handheld Data Preservation screen as shown below in Figure 5. Check <**Erase all application data>** to erase all data on the Blackberry device. If prompted, choose to not backup data files.
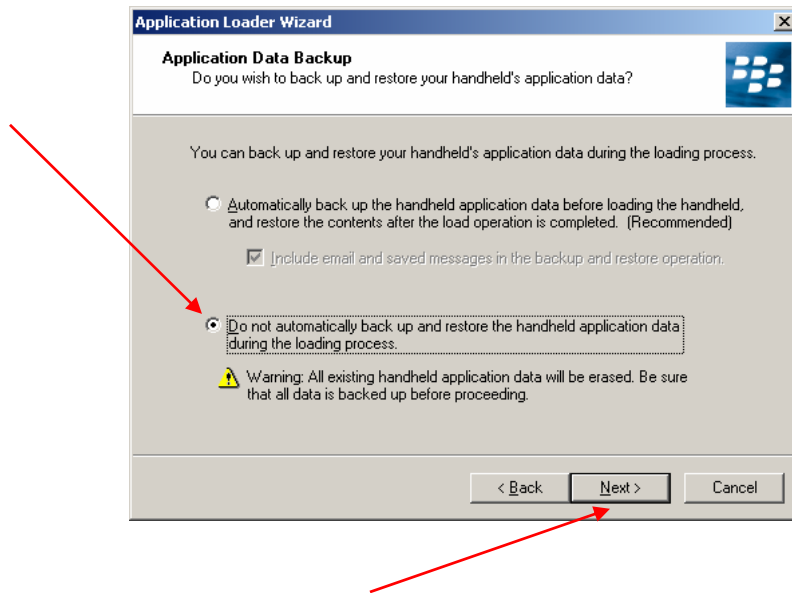

Figure 5. Erase Application Data

Then click <**Next>** to continue.

3.2.5 Application Data Backup

Select the <**Do not automatically backup and restore the handheld application data during the loading process>** option as shown below. When this option is selected it will erase all handheld data
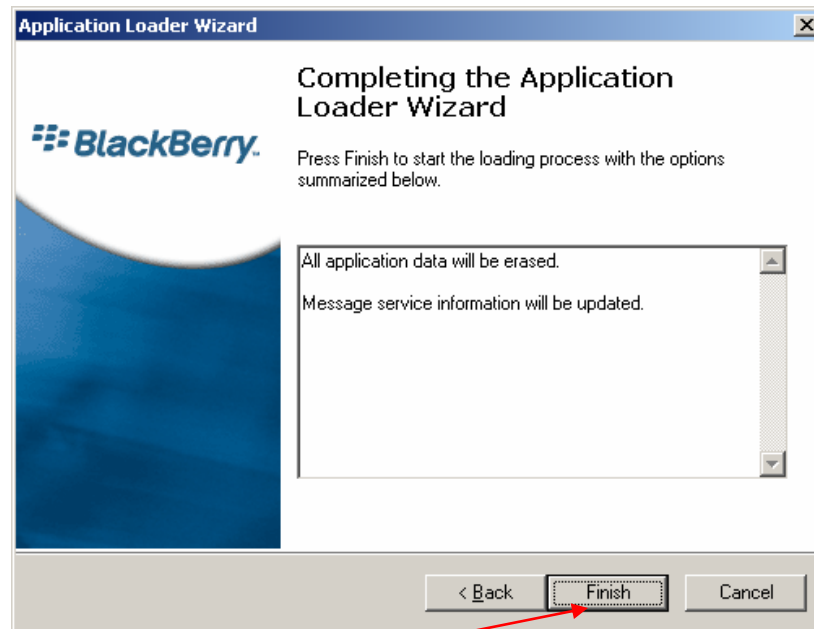

Figure 6. Backup Data

Then click <**Next>** to continue.

3.2.7 Completing the Loading of the Application Wizard

The next screen will be a warning screen stating that **All application data will be erased** as shown below in Figure 7.

Figure 7. Completing Application Loader

Click <**Finish>** to erase the data.

All application data will be erased from the BlackBerry. This also forces password expiration and clears any initial screen messages that the user set up previously. However, the calendar, tasks and notes etc. (except email messages) will resynchronize with Outlook and be placed back on the BlackBerry after the completion of this process.

The next screen, shown in Figure 8, requires no action on the users part.
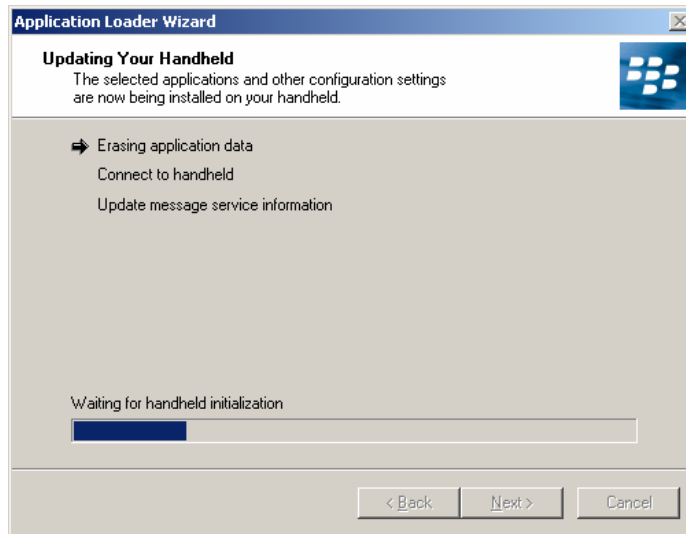
Figure 8. Updating Handheld

3.2.8   Completion of the Process

Once the process has completed a screen as shown in Figure 9, will notify the user of successful completion. The device is now cleared.

Figure 9. Process Completion
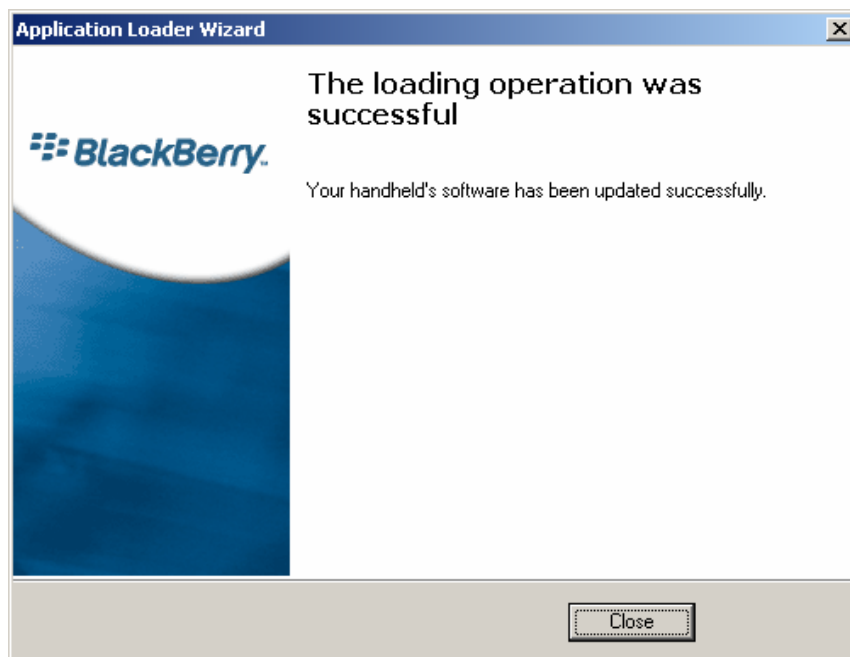
11

4.   Alternative Blackberry Clearing Processes

The following processes are purported to also clear data residing on a BlackBerry. They are included here for reference and may be used in lieu of the process described in Section 3.

4.1   The Erase Data and Disable Handheld Command

The **Erase Data and Disable Handheld** command is sent wirelessly to a BlackBerry device, erasing all of the device data and disabling it so that it can no longer be used on the BlackBerry Enterprise Server. When this command is sent, it should be verified by the sender that the command was received successfully.

4.1.1   Requirements

A BlackBerry device must be turned on and in an area of coverage to receive the command. If the device is turned off or out of coverage, the command is queued on the BlackBerry Enterprise Server until the device is turned on or returns to an area of coverage.

To be able to view and verify the success of the command, the BlackBerry Policy Service (POLC) logging level must be set to 4.

4.1.2   Sending the Erase Data and Disable Handheld Command

Complete the following steps:

(1)   Open **BlackBerry Manager**.
(2)   Go to the **User List** tab.
(3)   In the IT Admin section, click <**Erase Data and Disable Handheld>** in the list of IT commands.
          A dialog box appears, stating that all data will be erased if the user proceeds.
(4)   Select <**Proceed>.**

4.1.3   Determining the Success of the Command

To verify when the Erase Data and Disable Handheld command was sent and received, review the POLC log file (located by default in the BlackBerry Enterprise Server directory, in subfolder Logs/<date>.

Lines similar to the following appear in the POLC log file:

[40000] (10/03 13:00:52):{0x974}{username@domain.com,PIN=XXXXXXXX, UserID=1}SCS::PollDBQueueNewRequests - Queuing KILL_DEVICE_REQUEST request

The above line indicates when the command was first sent and that the command is being queued for the user.

[40000] (10/03 13:01:15) :{0x960} {username@domain.com, PIN=XXXXXXXX, UserId=1}RequestHandler::HandleITADMINDataCommand - ITPolicy Success Ack for the command KILL_HANDHELD_COMMAND - Processing packet, Tag=23980295

The above line indicates when the BlackBerry device received the command and that it sent a confirmation of the receipt.

Note: To search using a string in the log file, search for ITPolicy Success Ack for the command KILL_HANDHELD_COMMAND. Once it is located, verify the user associated with the command. Search for this string when the BlackBerry device does not meet the requirements to receive the command when it is first sent.

4.2   Erase all the Data and Applications on the BlackBerry Device

The following procedures will delete either all data, or all data and applications on the device. The choice can be made to either erase all the data or all the data and applications on the BlackBerry device.

To erase all the data:

(1)   Select the <**Wipe Handheld>** option.
(2)   Type an incorrect password ten times.
(3)   Use Application Loader to erase all data.
(4)   Use Backup and Restore to clear the device databases.

To erase all the data and applications:

(1)   Connect the device to the computer running Desktop Manager.
(2)   In Desktop Manager, double-click the <**Application Loader>** icon.
(3)   In the Application Loader Wizard window, click <**Next>**.
(4)   On the Device Security Password screen, type an incorrect password and click <**Next>**.
(5)   Perform this step ten times.
(6)   Click <**Close>**.

Without software the device is unresponsive. It displays device error 507. To re-install the device software, open the Application Loader and select the software and applications to install.

9/6/2006

4.3   Select the Wipe Handheld Option

To erase all the data on the BlackBerry device, complete the following steps. This option is available with BlackBerry Device Software 3.8 and later.

(1)   In the device options, click <**Security>**.
(2)   Click the trackwheel and select <**Wipe Handheld>**.
(3)   Click <**Continue>**.
(4)   Type <**blackberry>**. All the data on the BlackBerry device is erased.

4.4   Use Backup and Restore to Clear the Databases

To clear the databases on a BlackBerry device:

(1)   Connect the device to the computer running Desktop Manager.
(2)   In Desktop Manager, double-click the <**Backup and Restore>** icon, then click <**Advanced>**.
(3)   Press and hold the Shift key while selecting all the databases in the Handheld Databases list box.
(4)   Click <**Clear>**.
(5)   Click <**OK>** on the Warning window. All databases on the BlackBerry device are erased.
(6)   Click <**Close>** until the Desktop Manager is displayed.