Global Relief Technologies, LLC. Rapid Data Management Software (RDMS)

(Software Version: 2.3.0)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 0.3

Prepared for:

Global Relief Technologies, LLC.
40 Congress Street, Suite 300
Portsmouth, NH 03801 USA
Phone: (603) 422-7333
Fax: (603) 422-7331
http://www.globalrelieftech.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2/24/2006	Cas Stulberger	Initial draft
0.2	7/20/2006	Cas Stulberger	Updated according to initial lab questions
0.3	10/21/2006	Cas Stulberger	Updated User Roles Table 4 per lab guidance
1.0	12/22/2006	Cas Stulberger	Specifed key establishment strength and minor fixes

Table of Contents

Table of Figures

Table of Tables

0 Introduction

0.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Rapid Data Management Software (RDMS) from Global Relief Technologies, LLC (GRT). This Security Policy describes how the Rapid Data Management Software meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/cryptval/

The Rapid Data Management Software is referred to in this document as RDMS, the RDMS application, or the module.

0.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The GRT website (http://www.globalrelieftech.com) contains information on the full line of products from GRT.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

0.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to GRT. With the exception of this Non-Proprietary Security Policy and the user manual, the FIPS 140-2 Validation Documentation is proprietary to GRT and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact GRT.

1 Rapid Data Management Software

1.1 Overview

The Rapid Data Management Software (RDMS) is a software application developed by Global Relief Technologies (GRT) designed for installation on a Personal Digital Assistant (PDA) and cellular communications devices. The device is used during humanitarian and relief efforts in order to gather data and information quickly about the surrounding area to better decide where to allocate resources and what resources are needed.

The user of the device fills out a survey by answering a series of questions. When the survey is completed, it is saved to be edited or uploaded to the server later. The survey can be uploaded to the server when the device running RDMS is connected to an internet connection via a computer or a satellite uplink. The completed surveys are uploaded using Transport Layer Security (TLS) to the server in Portsmouth, New Hampshire. The server is part of the Virtual Network Operations Center (VNOC), which stores the uploaded surveys. A user accesses the VNOC via an https connection and can view all the uploaded surveys in order to help coordinate resources with humanitarian and relief efforts.

RDMS software is customized to meet a client's specific requirements for collecting data and uploading it to the server. The RDMS application runs on the Windows © Mobile 5.0 Operating System. RDMS includes mapping software and satellite imagery for navigational and data upload viewing purposes, which is stored on a Flash Card on the PDA and is accessed and manipulated using the MAPX software. RDMS uses this mapping software to provide GPS services, mapping and basic GIS functionality. RDMS also builds in industry-standard FIPS-approved cryptographic algorithms used to securely connect to the VNOC server using TLS.

The Rapid Data Management Software is validated at the following FIPS 140-2 Section levels:

Table 1 - Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	3
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

1.2 Module Interfaces

The Rapid Data Management Software is a Software module that meets overall level 1 FIPS 140-2 requirements. The cryptographic boundary of the Rapid Data Management Software is defined by the hard, opaque metal and plastic enclosure of the PDA. The logical cryptographic boundary of the module is composed of the RDMS software running on the Pocket PC Operating System. A Physical block diagram of the Pocket PC is shown in Figure 1.

The external connections of the PDA consist of the Alternating Current/Direct Current (AC/DC) Power Adapter, the Serial Port, and the Universal Serial Bus (USB) Port. The Serial and USB ports are used to connect the PDA to either a computer or a satellite uplink, which is then able to access the Internet in order to upload reports from the PDA to the server or download questionnaire updates from the server to the PDA. The touch screen and the buttons receive inputs from the user. The GPS Card and the 2 Gigabyte (GB) compact flash card are connected at the top of the PDA.

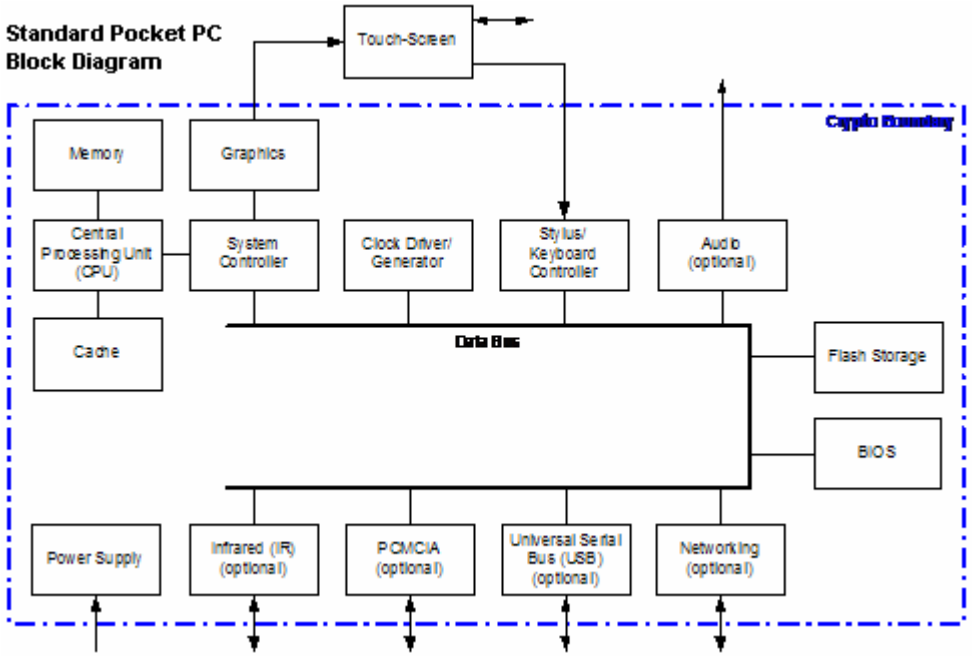

Figure 1 - Standard Pocket PC Physical Block Diagram

The touch screen is at the cryptographic module boundary and there is also a serial port within the boundary.

The AC/DC Power Adapter is shown below in Figure 2 - AC/DC Power Adapter. The AC/DC Power Adapter is used to charge the battery pack or deliver power to the PDA while the PDA is in use.

Figure 2 - AC/DC Power Adapter

The Serial Port connection is shown below in Figure 3 - Serial Port. The Serial Port is used to connect to the Internet in order to upload reports to the server or download questionnaire updates from the server.

Figure 3 - Serial Port

The USB Port connection is shown below in Figure 4 - USB Port. The USB Port is used to connect to the Internet in order to upload reports to the server or download questionnaire updates from the server.

Figure 4 - USB Port

The Touch Pad and Buttons are shown below in Figure 1 - Standard Pocket PC Physical Block Diagram. The Touch Pad and Buttons are used to input information to the PDA, select what menu to go to, initiate transmission of data to the server, etc.

Figure 5 - Touch Pad and Buttons

The back of the PDA is shown below in Figure 6 - Back of PDA.

Figure 6 - Back of PDA

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 2 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Rapid Data Management Software (RDMS) Port/Interface
Data Input	Touch Screen, Buttons, GPS Card, Serial Port, and USB Port
Data Output	Speakers, Display, Serial Port, and USB Port
Control Input	Touch Screen and Buttons

FIPS 140-2 Logical Interface	Rapid Data Management Software (RDMS) Port/Interface
Status Output	Display and Speakers
Power	Power Plug/Adapter

1.3 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role. The operator of the module assumes either of the roles based on the operations performed without any authentication. Both of the roles and their responsibilities are described below.

1.3.1 Crypto Officer Role

The Crypto Officer role has the ability to install and configure the module. Descriptions of the services available to the Crypto Officer role are provided in the table below.

Table 3 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP	Type of Access to CSP
Install	Installs RDMS and associated applications on the PDA	GRT Password, PRNG Seed, HMAC SHA-1 Integrity Check Key	Product installed	Enters default GRT password, and PRNG seed	Write
Uninstall	Uninstalls the software from the PDA	Uninstall Program Command	Product uninstalled	The RSA key is zeroized and removed from the module. Deleting InstallID.xml is part of the uninstall procedure and doing so zeroizes the GRT password, and PRNG seed	Write
Set Preferences	Sets up the Device ID, GPS Com Port, GPS Baud, Post URL, and Refresh URL	Preferences Menu Screen	New Preferences	None	None

1.3.2 User Role

The User role has the ability to Add Reports, Edit Reports, View Map, create Evacuation reports, and Transmit data to the server. Descriptions of the services available to the User role are provided in the table below.

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP	Type of Access to CSP
Add Report	Create and save a report	Click on the Add Report Button on the RDMS Main Menu	New report created	None	None
Edit Report	Edit a saved report	Click on the Edit Report Button on the RDMS Main Menu	Report Changed	None	None
View Map	View the maps stored in the 2GB memory card	Click on the Globe in the task bar at the bottom right of the screen	Map of current location displayed on the screen	None	None
Create Evacuation Report	Create an Evacuation report	Click on the Contact Button	Evacuation report created	None	None
Transmit Data	Connect to the server	Click on the Transmit Data button on the RDMS Main Menu	Successful transmission of reports or error connecting to server	TLS Symmetric Session Keys	Read
Send Evacuation Report	Transmit completed reports or Evacuation reports	Click the Send button on the Report Summary screen which can be accessed from the Contact button	Successful transmission of Evacuation report or error connecting to the server	TLS Symmetric Session Keys	Read
Download Questions	Download updated and new questions added by users to the PDA	Select Refresh Data from Server from the Preferences Menu on the RDMS Main Menu Screen	Questions loaded onto the PDA	None	None

1.3.3 Physical Security

Rapid Data Management Software is a multi-chip standalone cryptographic module.

The physical security requirements do not apply to this module, since it is a software module and does not implement any physical security mechanisms.

Although the module consists entirely of software, the FIPS 140-2 test platform is a standard Pocket PC which has been tested for and meets applicable Federal Communications Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home use.

1.3.4 Operational Environment

The module is to be tested on a PDA running Windows Mobile 5.0. The PDA is a single-user operating system and only a single operator can use the device at a time. The PDA shall not be configured to add additional networking services that would allow multi-operator capabilities, and GRT does not configure the device in this manner. Thus, the PDA is delivered as a single-user system, consistent with NIST guidance.

Refer to the CMVP document, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program Section 6.1 Single Operator Mode and Concurrent Operators page 36, for resolution on the issue of "Multi user" modes. This document is located at: http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf.

1.3.5 Cryptographic Key Management

The RDMS Application implements the following FIPS-approved algorithms:

- Deterministic Random Number Generator (RNG) – Appendix A.2.4 of ANSI X9.31 (certificate #205)
- HMAC SHA-1 – FIPS 198 (certificate #184)
- SHA-1 – FIPS 180-2 (certificate #478)
- Triple-DES CBC encrypt/decrypt – FIPS 46-3 (certificate #444)

Additionally, the module utilizes the following non-FIPS-approved algorithm implementation:

- RSA – 1024 bit encrypt (key wrapping; key establishment methodology provides 80 bits of encryption strength)
- OpenSSL non-approved RNG

The module supports the following critical security parameters:

Table 5 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP or Public Key	Key Type	Generation / Input	Output	Storage	Deletion	Use
TLS Symmetric Session Keys	3DES CBC	Generated internally	Exits electronically in encrypted form during TLS session negotiation	Stored in RAM for duration of the session	Deleted after session is over	Encrypting data transferred during TLS with the server
VNOC Server Public Key	1024 RSA public key	Input Electronically during TLS negotiations in an SSL server certificate	Never output	Stored in RAM for duration of the session	Deleted after session is over	Encrypts the session key so that only the server can decrypt it with its private key
Default GRT Password	Password / PIN	Electronically entered in plaintext	Never output	Stored in InstallD.xml	Uninstalling the module or overwriting	Accessing the settings in User Preferences
PRNG seed	8 bytes of seed value	Internally generated	Never output	Stored in RAM in plaintext	Upon restart of the RDMS application	Produce FIPS approved RNG seed

1.3.6 Self-Tests

In order to prevent any plaintext data from being inadvertently released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly.

The Rapid Data Management Software performs the following self-tests at power-up:

- Software Integrity Check - Verifies the integrity of the RDMS application by checking a HMAC SHA-1 computed over it.
- Known Answer Tests (KATs)
    - Triple-DES encrypt/decrypt KAT
    - RSA pairwise consistency check
    - HMAC SHA-1 KAT
    - X9.31 Appendix A.2.4 RNG KAT

The Rapid Data Management Software performs the following conditional self-tests:

- Continuous Random Number Generator Test for FIPS 140-2 approved ANSI X9.31 Appendix A.2.4 PRNG
- Continuous Random Number Generator Test for entropy gathering

The Software Integrity Check and the KATs are performed on initialization of the RDMS application. If the Software Integrity Check, the KATs, or the Continuous Random Number Generator Tests for entropy gathering fail, the user is alerted via a pop up message box and the RDMS application stops loading and exits. When the Continuous Random Number Generator Test for the FIPS 140-2 approved ANSI X9.31 Appendix A.2.4 PRNG fails, an error value is returned and an Upload Failed Message is displayed.

1.3.7 Design Assurance

Global Relief Technologies, LLC. utilizes Microsoft Visual Source Safe (VSS) version 6.0d to provide configuration management for the Rapid Data Management Software source code. User manuals are customized on a per client basis and are updated with each new version of Rapid Data Management Software.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the Rapid Data Management Software's FIPS documentation. This software provides access control, versioning, and logging.

1.3.8 Mitigation of Other Attacks

This section is not applicable. The module does not mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

2 Secure Operation

The Rapid Data Management Software meets Level 1 requirements for FIPS 140-2. The PDA always operates in single user mode since only one person may be using the PDA at a time and since all networking capabilities are disabled by GRT.

2.1 Initial Setup

RDMS and the associated programs necessary for the application to function are loaded onto the PDA by GRT. Nothing needs to be configured by the user since the PDA is always operating in FIPS approved mode.

2.2 Crypto Officer Guidance

The Crypto Officer is responsible for installing and uninstalling the software on the PDA, setting the preferences in the User Preferences Menu, and installing the PRNG seed and Software Integrity Key and password in InstallID.xml.

2.2.1 Initialization

The software module will be provided to the users by Global Relief Technologies, LLC. The software module is installed on the PDA along with the other programs necessary for it to operate.

Before installing the module, the operator needs to ensure that the system runs the specified operating system. The module must be installed, configured, and started before operators may utilize its features.

2.2.2 Management

The Crypto Officer does not perform any management on the PDA or the RDMS application after installation and configuration. The Crypto Officer however is responsible for uninstalling the RDMS application from the PDA during which the RSA key is zeroized and removed from the module.

2.2.3 Zeroization

The Symmetric key and the Server public key are temporary keys and are deleted after the communication session between the PDA and the Server is over.

2.3 User Guidance

The User accesses the module's cryptographic functionalities. Although the User does not have any ability to modify the configuration of the module, they should check that the host application is enabled and providing cryptographic protection.

3 Acronyms

Table 6 - Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AC/DC	Alternating Current / Direct Current
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
CMVP	Cryptographic Module Validation Program
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GB	Gigabyte
GIS	Global Information System
GPS	Global Positioning System
GRT	Global Relief Technologies
HMAC	(Keyed-) Hash MAC
ID	Identification
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PRNG	Pseudo-Random Number Generator
RAM	Random Access Memory
RDMS	Rapid Data Management Software
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VNOC	Virtual Network Operations Center

Acronym	Definition
VSS	Visual Source Safe