DIGITALGLOBE HEADQUARTERS
1601 DRY CREEK DRIVE, SUITE 260 ♦ LONGMONT, COLORADO 80503
303-684-4000 ♦ 303-684-4048 FAX ♦ www.digitalglobe.com

DigitalGlobe, Inc. WorldView Wideband Transmitter Security Policy

Release Version

Technical Note

Date: Jun. 22, 06

	Name	Date
Prepared by:	Skip Cubbedge	2/10/06
Testers		
Approved and Released by:		
Verified by:		

DIGITALGLOBE HEADQUARTERS
1601 DRY CREEK DRIVE, SUITE 260 ♦ LONGMONT, COLORADO 80503
303-684-4000 ♦ 303-684-4048 FAX ♦ www.digitalglobe.com

Change Record

Issue	Date	Section(s)	Description of Change	PCR No
1.0	2/10/06	All	Initial Release	

Table of Contents

DIGITALGLOBE HEADQUARTERS
1601 DRY CREEK DRIVE, SUITE 260 ♦ LONGMONT, COLORADO 80503
303-684-4000 ♦ 303-684-4048 FAX ♦ www.digitalglobe.com

WorldView Wideband Transmitter FIPS 140-2 Security Policy

Introduction

This document describes the security policy for the WorldView Wideband Data Transmitter (WBTx) Encryption Module, to meet FIPS 140-2 security requirements.

The WBTx is a self-contained component that incorporates FIPS-approved Advanced Encryption Standard (AES) encryption. The WBTx flies as a component on-board the WorldView satellite in a low-earth orbit (LEO). The image data and associated key material is considered by DG to be unclassified but company sensitive.

Cryptographic Module and Cryptographic Boundary

The cryptographic module is an implementation in VHDL of the AES algorithm, and is realized in an electronic integrated circuit that resides in the WBTx. The cryptographic boundary is defined to be the physical perimeter of the integrated circuit and the set of input and output pins of the circuit provide the physical input and output ports (across which logical paths of information flow). This module is a single-chip module. As a level 1 module, the WBTx provides no physical security, and though not included in the scope of FIPS validation, when assembled, its box enclosure along with the satellite's in-orbit distance from Earth provide physical security.

Roles

The WBTx, in concert with the trusted uplink path, implements User and Crypto Officer roles. Only persons who are trained and accredited DigitalGlobe Satellite Operators are authorized to act in these roles. DG Satellite Operators must pass special training before functioning in this role, and must also sign a COMSEC briefing before handling key material.

Single Operator

The WBTx runs in Single User Mode. Multiple concurrent operators are not supported.

User

The User role is defined as a DG Satellite Operator receiving image data that has been encrypted by the WBTx.

Crypto Officer

The Crypto Officer role is defined as a DG Satellite Operator loading keys into the WBTx, controlling the bypass mode of the WBTx, and observing status telemetry from the WBTx.

Services

The cryptographic services of the WBTx consist of the encrypted wideband downlink data, the key loading interface, and the control and status information of the WBTx related to the AES implementation. All services provided by the module are described in this section, and the operator has access to all of these services.

Overview of Functions and Modes of Operation

The WBTx operates in a FIPS-approved mode only when the cryptographic bypass function is disabled. When the cryptographic bypass function is enabled, the WBTx operates in a non-approved mode.

Function Descriptions

Wideband Data Encryption

The WBTx AES module provides the following FIPS 140-2 approved algorithms:

> **Encryption:** AES, as described in FIPS PUB 197, in 128-bit key Electronic Codebook Mode, as described in NIST SP 800-38a. Performed only on wideband image data as provided to the WBTx by the satellite data recorders.

Key Management

The WBTx performs limited key management, as described below.

Key Generation

The WBTx does not provide key generation. All keys must be entered by the Crypto Officer role.

Self-Tests

The wideband downlink system performs a procedural self test at each power-on of the WBTx, which occurs at the beginning of each satellite contact.

User Guidance

The User is responsible for using the WBTx encryption module to encrypt data prior to downlink transmission. On each downlinking event, the User shall verify in telemetry that the uploaded key is selected, prior to commencing downlink transmission. In addition, the User shall verify from telemetry that the Bypass mode of the WBTx encryption module is not engaged, in order to ensure that the WBTx is correctly operating in FIPS-approved mode.

Crypto Officer Guidance

The Crypto Officer is responsible for key management, controlling the cryptographic bypass, and managing faults of the WBTx encryption module. Keys shall be uploaded by the Crypto Officer to the WBTx using only the trusted path.

Miscellaneous

Mitigation of Specific Attacks

The WBTx is not designed to mitigate specific attacks.

Delivery and Operation

The WBTx is considered to be delivered to DigitalGlobe when it has been installed on the spacecraft during the spacecraft integration and test procedure. From that point on the WBTx is considered to be in its operational configuration.

Tabular Summaries

As required by FIPS 140-2 Derived Test Requirements, here are tables summarizing certain aspects of the security policy:

Role	Type of Authentication	Authentication Data
User	None	N/A
Crypto Officer	None	N/A

Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
User	None
Crypto Officer	None

Strengths of Authentication Mechanisms

Role	Authorized Services
User	Encrypt Data
Crypto officer	Upload Keys, Control Bypass, Reset/Zeroize

Services Authorized for All Roles

Service	Cryptographic Keys and Critical Security Parameters	Type(s) of Access (e.g., Read, Write, Execute)
Upload Key	Upload Encryption Key	Crypto Officer Write
Encrypt	Upload Encryption Key	User Execute
Reset	Encryption Key Zeroized	Crypto Officer Execute, Write

Access Rights Within Services