Symmetry

Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Revision 0.7, 9 April 2010

G4S Technology Limited
Challenge House,
International Drive,
Tewkesbury, Gloucestershire
GL20 8UQ

1 Revision History

Date	Revision	Description
29 October 2009	0.1	Initial version
4 February 2010	0.2	Modified to address changes to Integrity checking mechanism
24 February 2010	0.3	Modified to reflect company name change
5 March 2010	0.4	Name change and installation instructions
26 Mach 2010	0.5	Modified in response to lab comments
29 March 2010	0.6	Updated software version number
9 April 2010	0.7	Modified in response to lab comments

Table of Contents

Table of Figures

2 INTRODUCTION

2.1 Security Policy, Product and Evaluation Identification

Security Policy Title: Symmetry Cryptographic Module Security Policy

Security Policy Version: Version 0.7

Product Identification: Symmetry Cryptographic Module version 1.2.0.0

FIPS Validation: FIPS 140-2

Security Level: 1

2.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the Symmetry Cryptographic Module, also referred to as "the module" within this document. This Security Policy details the secure operation of the Symmetry Cryptographic Module as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

2.3 References

For more information on the Symmetry Cryptographic Module please visit: http://www.g4stechnology.co.uk/Products/Smart-Card-Biometrics.aspx. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

2.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be G4S Technology Limited proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact G4S Technology Limited

3 Symmetry Cryptographic Module

The Symmetry Cryptographic Module (SW Version 1.2.0.0), also referred to simply as “module”, is a Software-only module that resides on a General Purpose Computer (see Figure 1).

In simple terms, the Symmetry Cryptographic Module provides data encryption functionality to enable its client application to provide a secure data channel to transfer data securely over a network.

The cryptographic boundary of the module is the case of the Personal Computer (PC) on which it is installed. See Figure 1. The module is a software module running on a standard General Purpose Computing (GPC) device. The processor of the GPC device executes all software. All software components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

The cryptographic module is packaged as a dynamic-link library (DLL) and a separate MAC (message authentication code) file used by the DLL in its startup software integrity test.

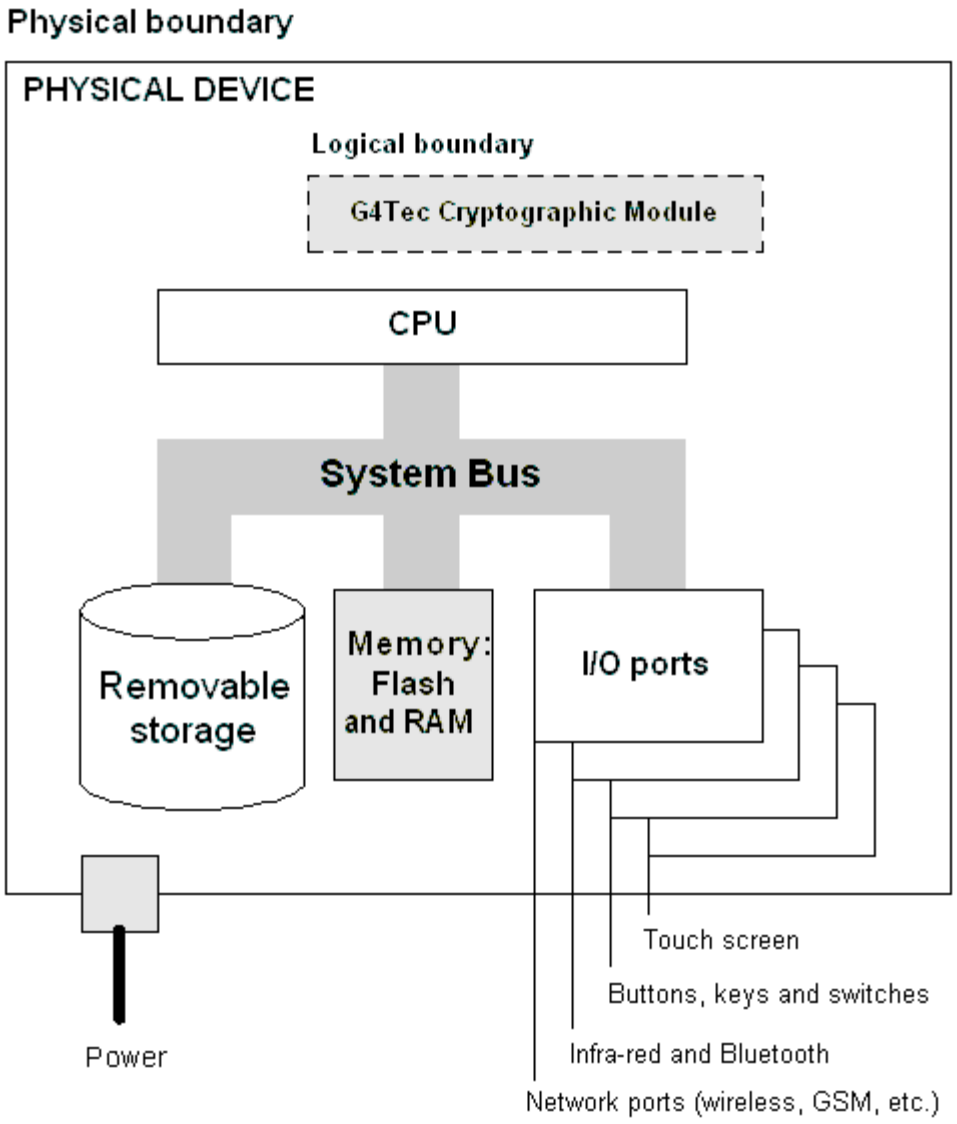

Figure 1: Block Diagram of the cryptographic boundary

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	**1**
Module Ports and Interfaces	**1**
Roles, Services and Authentication	**1**
Finite State Model	**1**
Physical Security	**N/A**
Operational Environment	**1**
Cryptographic Key Management	**1**
EMI/EMC	**1**
Self-Tests	**1**
Design Assurance	**1**
Mitigation of Other Attacks	**N/A**

Figure 2: Security Level specification per individual areas of FIPS 140-2

3.1 Module Interfaces

The Symmetry Cryptographic Module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the device on which it is installed. The device shall be running a supported operating system (OS) and supporting all standard interfaces, including keyboard, mouse, and data ports.

The Symmetry Cryptographic Module provides a logical interface via an Application Programming Interface (API). This logical interface exposes services (described in section 3.3) that the User may utilize directly.

The logical interfaces provided by the Symmetry Cryptographic Module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

- Data Input – Input to all API functions
- Data Output – Output from all API functions
- Control Input – API function calls
- Status Output – Return codes from API function GetEncryptionModuleStatus()

3.2 Operational Environment

The Symmetry Cryptographic Module has been tested on and found to be conformant with the requirements of FIPS 140-2 overall Level 1 on the following GPC operating systems:

- Windows XP Professional SP3 (x86),
- Microsoft Windows Vista SP2 (x86),
- Microsoft Windows 7 (x86),
- Microsoft Windows Server 2003 SP2 (x86)
- Microsoft Windows Server 2008 SP2 (x86)

The cryptographic module runs in its own operating system threads. This provides it with protection from all other processes, preventing access to all keys, intermediate key generation values, and other CSPs.

The task scheduler and architecture of the operating system maintain the integrity of the cryptographic module.

The module supports only one single user and only one operator can have access to the device that contains the module at a time.

3.3 Roles and Services

The Symmetry Cryptographic Module implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Figure 4 summarizes the services available to each role.

Role	Description
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Figure 3: Roles

3.4 Access to Services

The following table, Figure 4, lists the authorized services linked to each of the Roles offered by the module.

Crypto-Officer	User	Authorized Services	Description
X		LoadDataKey	Loads a Data Encryption Key into the module
X	X	LoadIV	Loads an IV into the module
X	X	EncryptData	Encrypts data using AES-256 in CBC mode.
X	X	DecryptData	Decrypts data using AES-256 in CBC mode.
X		ZeroDataKey	Overwrites the Data Encryption Key with zeros to delete it.
X	X	RunSelfTests	Performs all FIPS 140-2 defined self tests.
X	X	GetEncryptionModuleStatus	Returns the status of the module

Figure 4: Services Authorized for Roles

3.5 Physical Security

The Symmetry Cryptographic Module is a software only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

3.6 Cryptographic Key Management

The following tables list all keys used within the Symmetry Cryptographic Module module. Currently, AES-256 is the only Approved encryption algorithm in the Symmetry Cryptographic Module product and all encryption keys are AES-256 keys.

Key type	Purpose
Data Encryption Key	To encrypt and decrypt module data as appropriate.

Figure 5: Keys used by the Symmetry Cryptographic Module

3.6.1 Key generation

The Symmetry Cryptographic Module does not generate key material or CSPs.

3.6.2 Key entry and output

The module supports the following key entry:

- The Data Encryption Key is loaded into the module in plaintext form via the LoadDataKey service.

3.6.3 Key storage

Key material is stored in the Symmetry Cryptographic Module in volatile local GPC storage.

3.6.4 Zeroization of key material

The Data Encryption Key can be zeroed by calling the ZeroDataKey service.

3.6.5 Access to key material

The following matrix (Figure 6) show the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

Service	Data Encryption Key
LoadDataKey	W
LoadIV	
EncryptData	R
DecryptData	R
ZeroDataKey	W
RunSelfTests	
GetEncryptionModuleStatus	

Figure 6: Key Access

Access rights

Blank Not Applicable
W Write access
R Read Access

3.7 Cryptographic Algorithms

The Symmetry Cryptographic Module supports the AES-256 (cert #1314) FIPS-approved algorithm and the SHA-1 (cert #1202) and HMAC (cert #765) FIPS approved algorithm (in the Software Integrity Test). There are no non-FIPS-approved algorithms within the module.

3.8 Self-Tests

The Symmetry Cryptographic Module implements both power-up and conditional self tests as required by FIPS 140-2. The following two sections outline the tests that are performed.

3.8.1 Power-up self-tests

The following table, Figure 9, lists the power-up self-tests performed by the module:

AES-256 known answer test
Software integrity test (HMAC)

Figure 7: Power-up Self-tests

Each of these tests is executed when the computer is turned on and the module first executes. If any of these tests fail, the module will not load. The module must be reset to re-execute these tests.

3.8.2 Conditional self-tests

There is a load key test performed whenever a Data Encryption Key is loaded into the module. Two copies of the key are provided to the LoadDataKey service. This test compares the two copies of the key, and fails if they are different. If the test fails, the test returns an error and the module enters a non-operational state. The test is performed as an added assurance to guard against errors introduced in key transport, but is not required by the FIPS 140-2 requirements.

3.9 Design Assurance

G4S Technology Limited employ industry standard best practices in the design, development, production and maintenance of the Symmetry Cryptographic Module product, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas

throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

3.10 Installation and Use

The module binary is a Windows DLL. It is always in its FIPS approved mode of operation. To set up the module, a key must be loaded with the LoadDataKey service. Then an IV can be added with the LoadIV service. Then the module is ready to encrypt and decrypt data with the EncryptData and DecryptData services.

3.11 Mitigation of Other Attacks

The module does not mitigate other attacks.