

---

My Product  
Cygnacom Solutions

**FIPS 140-2 Non-Proprietary  
Security Policy**

**Level 2 Validation**

**July 2002**

# Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1	PURPOSE .....	3
1.2	REFERENCES .....	3
<b>2</b>	<b>MY PRODUCT.....</b>	<b>4</b>
2.1	MODULE PORTS AND INTERFACES .....	4
2.2	ROLES AND SERVICES .....	4
2.3	FINITE STATE MODEL .....	5
2.4	PHYSICAL SECURITY .....	5
2.5	CRYPTOGRAPHIC KEY MANAGEMENT .....	5
2.6	EMI/EMC .....	5
2.7	SELF-TEST .....	6
2.8	DESIGN ASSURANCE .....	6
2.9	APPROVED MODE OF OPERATION .....	6

# 1 INTRODUCTION

## *1.1 Purpose*

This is a non-proprietary FIPS 140-2 Security Policy for MyProduct. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 2 requirements. This Policy forms a part of the submission package to the validating lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard visit <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

## *1.2 References*

This Security Policy describes how this module complies with the eleven sections of the standard.

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at <http://csrc.nist.gov/cryptval/>.
- For more information about Cygnacom Solutions please visit <http://www.entrust.com/entrustcygnacom/index.htm>.

## 2 My Product

Cygnacom Solutions' My Product is a crypto accelerator. It has many features and supports AES, 3 DES, RSA etc..... The boundary is defined as the box in which the accelerator is located and there are no exclusions from the module. The block diagram for the module is as shown below with all the inter-connections between the components of the module.

The module implements DES (Legacy Purposes), 3 DES, AES and RSA (signing/verification) algorithms in the approved mode. The module also implements RC6, MD5 in the non approved mode.

### 2.1 Module Ports and Interfaces

The module is considered to be a multi chip standalone module. The module has the following interfaces

- Data Input interface: The network interface card is defined as the data input interface through which data is input to the module.
- Data Output Interface: As the module is being validated for level 2 requirements, the network interface card is defined as the data output interface.
- Control input interface
- Status output interface: LEDs' on the front and the back of the module are status output interfaces.

The below table describes the relationship between the logical and physical interfaces.

	Logical Interface	Physical Interface
Data input interface		
Data output interface		
Control input interface		
Status output interface		
Power interface		

Table 1 – Mapping Physical and Logical Interfaces

### 2.2 Roles and Services

The module supports a Crypto Officer and an User role. The module implements role based authentication using passwords and keys. Initial authentication to the module is controlled by a factory set password which the CO uses to authenticate to the module and to configure it. The module doesn't support a maintenance role.

The services available to the CO are

- Initialization of the module
- Create User roles
- Generate and Zeroize the keys
- Perform crypto operations

User can perform

- Generate and Zeroize keys
- Perform crypto operations

The below table shows the services available to each role.

The module implements role based authentication using passwords or keys. The strength of this authentication mechanism is dependent on the length of the password and the module implements good password generation principles.

### **2.3 Finite State Model**

The module has been designed to meet the requirements of the FSM. A detailed FSM has been submitted as part of the validation process to the lab. The module consists of the following states: Power Off, Power On, Self Tests, Key generation, Key entry, Key output, CO and User, Error states.

### **2.4 Physical Security**

The module is defined as a multi chip standalone module. The module consists of production grade components which include standard passivation techniques. The manufacturing process of the module is defined in great detail in Document A. As the module is being validated for level 2 requirements, the module has tamper evident seals across the module as shown below.

### **2.5 Cryptographic Key Management**

The following table summaries the module's keys:

Key	Generation	Storage	Use
DES			
3DES			
AES			

The module stores the keys internally in encrypted form and the keys are decrypted when a user logons to the module using authentication data. The 3DES MAC key is also hardcoded with in the module and is zeroized by destroying the module.

### **2.6 EMI/EMC**

The module complies with EMI/EMC requirements as specified by 47 code of federal regulations, Part 15 Subpart B. The module was tested by "Their Labs" with FCC number 123456. The compliance certificate is submitted to the lab as part of the validation process.

## **2.7 Self-Test**

The module performs the following self tests:

**Software Integrity Tests:** The module checks the integrity of its various components using 3DES-MACs.

**Cryptographic Algorithm KATs:** Known Answer Tests (KATs) are run at power-up for the DES, Triple DES and AES (CBC mode) encryption/decryption, RSA digital signature signing/verifying.

## **2.8 Design Assurance**

The module satisfies the design assurance requirement as described in the standards by adopting the following methodologies.

## **2.9 Approved Mode of Operation**

To operate the module in approved mode the CO has to configure the module in the following manner.