BASICS IP PC104
Security Policy

Version: 1.2

Vocality International Ltd.

Revision Date: 1 June 2012

Contents

Tables

Figures

1 Module Overview

The Vocality BASICS IP PC104 (hereafter referred to as the module) is a multi-chip embedded cryptographic module to be used as a router appliance. BASICS is the essential toolbox, offering a simplified approach to the deployment of networking and IP solutions. The module provides a number of ports for connection to an IP WAN such as a satellite modem. Designed for applications where efficiency is critical – power, space, or bandwidth – BASICS provides specific applications for every day challenges in system deployment.

The boundary of the module is defined as the outer perimeter of the module's metal enclosure. This module only functions within another enclosure.

Figure 1 – Image of the Cryptographic Module

The configuration of hardware and firmware for this validation is:

Hardware: 68551-01-1/68551C6

Firmware: Version 08_42.05

Figure 2 depicts the logical block diagram for the BASICS IP PC104 with the cryptographic boundary shown in red.

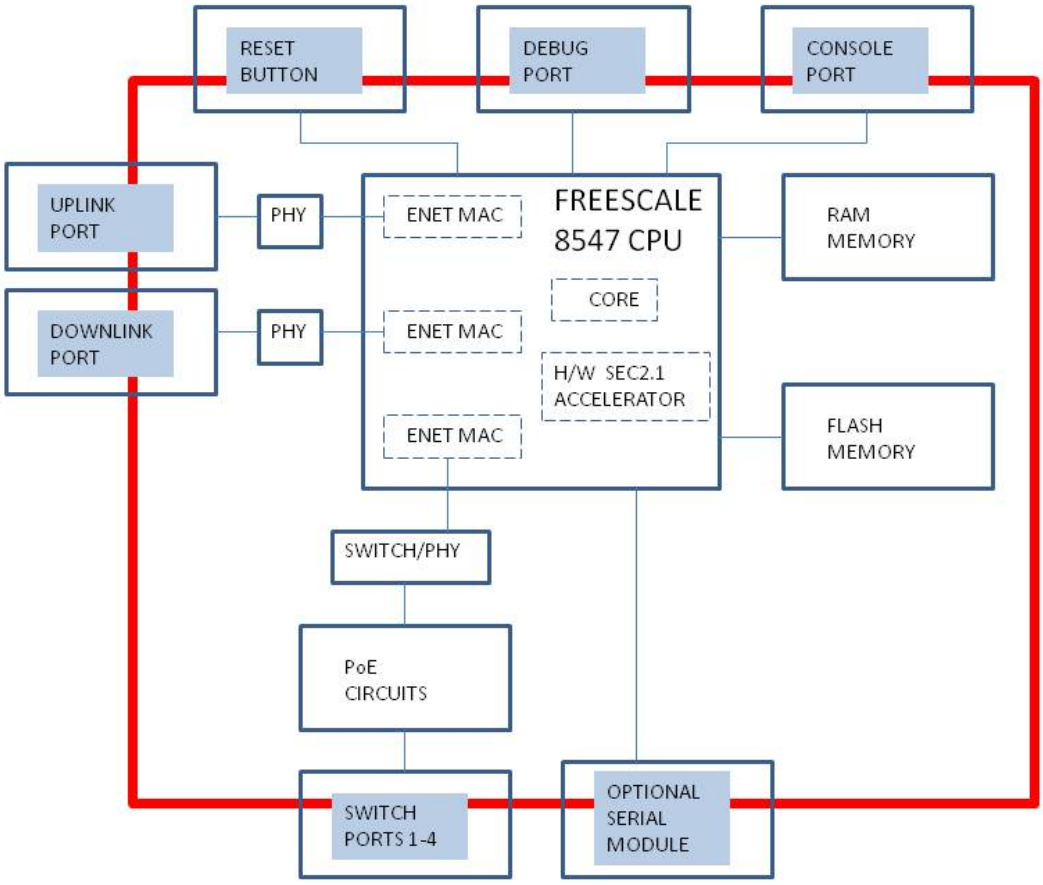

Figure 2 - Logical Block Diagram

Module services are described in Section 6 below.

The following non-security relevant component types have been excluded from the requirements of FIPS 140-2:

- Resistors (Qty. 24)
- Capacitors (Qty. 11)

2 Security Level

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

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

The module provides both a FIPS Approved mode of operation and a non-Approved mode of operation, comprising all services described in Section 6 below.

The module will enter FIPS Approved mode following successful power up initialization and configuration per the rules specified in Section 8 below. If a security rule is violated, the module will output an alarm indicating that the module is no longer operating in the Approved mode of operation.. The alarms can be viewed by looking at the “current alarms” page to see if the FIPS L2 MODE alarm is raised. The diagnostics configuration log contains details of which parameters are not configured in a FIPS Approved mode.

3.2 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 - FIPS Approved Algorithms

FIPS Approved Algorithm	CAVP Cert. #
AES Encrypt/Decrypt 128, 192, 256 (ECB, CBC, CTR modes)	1734
AES CCM (128, 192, 256 bits)	1734
AES CMAC	1734
AES GCM	1734
3-key Triple DES Encrypt/Decrypt	1123
DSA 1024 PQG Gen/Ver, Sig Gen/Ver, Key Gen.	540
ECDSA key generation, PKV, signature generation and verification (Curves P: 192, 224, 256, 384, 512)	226
RSA key generation (1024, 1536, 2048, 3072 and 4096), signature generation and verification (1024, 1536, 2048)	857
FIPS 186-2 RNG	923
HMAC-SHA-1, 224, 256, 384, 512	1010
SHA-1, 224, 256, 384, 512	1518

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode.

Table 3 – FIPS Allowed Algorithms

FIPS Allowed Algorithm
Diffie-Hellman (for key agreement; provides 80 or 112 bits of encryption strength)
RSA Key Wrapping (provides between 80 and 112 bits of encryption strength)
ECDH (for key agreement; provides between 80 and 256 bits of encryption strength)
NDRNG

4 Ports and Interfaces

The BASICS IP PC104 is a multi-chip embedded cryptographic module with ports and interfaces as shown below.

Table 4 - Module FIPS 140-2 Ports and Interfaces

Port	FIPS 140-2 Designation	Name and Description
DC Power	Power	Power port
Power over Ethernet	Power	Power over Ethernet
Monitor and Control	Control input, Status output	10 pin connector to support RS232 and Status LED's
Ethernet (Uplink)	Data input, Data output	10 pin connector used to support an Ethernet interface
Ethernet (Downlink)	Data input, Data output	10 pin connector used to support an Ethernet interface
Ethernet	Data input, Data output	34 pin connector used to support 4 Ethernet interfaces
Reset Button	Control input	Restores the module to factory defaults

5 Identification and Authentication Policy

5.1 Assumption of Roles

The module supports three distinct operator roles, Administrator (CO), Read Only User and Read/Write User. The cryptographic module enforces the separation of roles using identity-based authentication via a unique username and password.

Table 5 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
Administrator (CO)	This role has read/write privileges to the module including the configuration of User accounts and cryptographic keys.	Identity-based operator authentication	Username and Password
Read Only User	This role has read only privileges to the module except for the cryptographic keys which are not accessible.	Identity-based operator authentication	Username and Password
Read/Write User	This role has read/write privileges to the module except for configuration of User accounts and cryptographic keys.	Identity-based operator authentication	Username and Password

Table 6 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username/Password	The username is between 1 and 16 characters in length chosen from a set of 92 possible characters. The password is between 6 and 32 characters in length chosen from a set of 92 possible characters (alphanumeric, including special characters). Therefore the minimum username/password combined length is 7 characters and the probability that a single random attempt will succeed or a false acceptance will occur is 1/(92^7) which is less than 1/1,000,000. Authentication attempts may be made over the console port or via SSH. The console port operates at 9600bps. A minimum of 9

	characters (72bits) must be entered for each authentication attempt (1 for username, 6 for password and 2 carriage returns). The most authentication attempts theoretically possible in one minute over the console port is (60*(9600/72)) 8000. Therefore the probability of successfully authenticating to the module within one minute is 8000/(92^7), which is less than 1 in 100,000. The fastest link speed that the SSH sessions can operate over is 100Mbps Ethernet, which allow a maximum packet per second rate of 148800. A minimum of 2 packets is required for each authentication attempt (one for the username and one for the password – in practice there are many more packets involved in establishing the SSH session). This allows a theoretical maximum of 74400 authentication attempts per second. Therefore the probability of successfully authenticating to the module within one minute is (60*74400)/(92^7), which is less than 1 in 100,000

6 Access Control Policy

6.1 Roles and Services

Table 7 - Authenticated Services

Role(s)	Service	Description
Administrator	Add/Delete/Manage Users	Adds or removes Read Only and Read/Write Users and all parameters associated with User accounts
Administrator	Configure SSH, SNMP, and IPSec	Enter Keys, Select Algorithms to be used with SSH, SNMP, IPSec. Configure security associations to be used with IPSec.
Administrator, Read/Write User	Configuration Dump	Output configuration data, including keys and authentication data in cipher text, into a config. file
Administrator, Read/Write User	Unit Configuration	Configure all other parameters not related to SSH, SNMP, IPSec key management (eg. Configure IP address, IP routing, alarm management, service management, etc.)
Administrator	FW Update	Updates the module's firmware
Read Only User	View Configuration details	Views configuration details not related to SSH, SNMP, IPSec key management
Administrator, Read/Write User, Read Only User	Get Status	View Statistics and status of module operations

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 8 - Unauthenticated Services

Service	Description
Self-Tests	Performed by power cycling the module
Configuration Reset	Returns the module to factory defaults

6.3 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 9 - Private Keys and CSPs

Key Name	Type	Description
IPSec Encryption Key	AES, TDES	Used by IPSec for data encryption
IPSec Integrity Key	HMAC-SHA-1	Used by IPSec for data integrity
IKE Pre-shared Key	AES, TDES	Used during the IKE protocol to establish cryptographic keys to be used by IKE.
IKE Encryption Key	AES, TDES	Used for peer-to-peer message encryption
IKE Integrity Key	HMAC-SHA-1	Used by IKE for data integrity
IKE Private Key	RSA, DSA, ECDSA	Used in IKE identity authentication
SSH Host Private Key	RSA, DSA, ECDSA	Used to create digital signatures
SSH Encryption Key	AES, TDES	Used to encrypt SSH traffic
SSH Integrity Key	HMAC-SHA-1	Used by SSH for data integrity
Diffie Hellman Private Key Components	DH	Used during DH Key agreement protocol
Seed and Seed Key	N/A	Used to initialize the Approved RNG
Administrator (CO) Password	Password	Used to authenticate the Administrator (CO)
Read/Write User Password	Password	Used to authenticate the Read/Write User
Read Only User Password	Password	Used to authenticate the Read Only User
Configuration Encryption Key	AES	Used to encrypt all other CSPs in stored and outputted configurations

6.4 Definition of Public Keys

The module contains the following public keys:

Table 10 - Public Keys

Key Name	Type	Description
FW Upgrade Public Key	RSA	Used to verify RSA signatures over firmware images
SSH Host Public Key	RSA, DSA, ECDSA	Used by SSH Client to verify digital signatures
SSH Client Public Key	RSA, DSA, ECDSA	Used by the device to verify digital signatures
Diffie Hellman Public Key Components	DH	Used by the DH Key Agreement protocol

6.5 Definition of CSPs Modes of Access

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- **G** = Generate: The module generates the CSP.
- **R** = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- **W** = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- **Z** = Zeroize: The module zeroizes the CSP.

Table 11 - CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
Administrator	Add/Delete/Manage Users	W, Z W, Z W, Z	Administrator (CO) Password Read/Write User Password Read Only User Password
Administrator	Configure SSH, SNMP, and IPSec	W, Z W, Z W, Z G, Z R, Z R, W, Z W, Z	IPSec Encryption Key IPSec Integrity Key IKE Pre-shared Key SSH Host Private Key SSH Host Public Key SSH Client Public Key Configuration Encryption Key
Administrator, Read/Write User	Configuration Dump	N/A	N/A
Administrator, Read/Write User	Configure Unit	N/A	N/A
Administrator	FW Update	R	FW Upgrade Public Key
Read Only User	View Configuration details	N/A	N/A
Administrator, Read/Write User, Read Only User	Get Status	N/A	N/A
N/A	Self-Tests	N/A	N/A
N/A	Configuration Reset	Z	All Keys and CSPs

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module does not contain a modifiable operational environment.

8 Security Rules

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide three distinct operator roles. These are the Administrator (CO) role, the Read/Write User role, and the Read Only User role.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. Until the time that successful authentication has taken place and an operator has been placed in a valid role, the module shall not grant access to any cryptographic services.
5. The cryptographic module shall perform the following tests.

   A. Power up Self-Tests

      1. Cryptographic algorithm tests
         - AES-ECB, CBC, CCM, CMAC, CTR, GCM Known Answer Test
         - Triple-DES Known Answer Test
         - HMAC-SHA-1 Known Answer Test
         - HMAC-SHA-224 Known Answer Test
         - HMAC-SHA-256 Known Answer Test
         - HMAC-SHA-384 Known Answer Test
         - HMAC-SHA-512 Known Answer Test
         - SHA-1 Known Answer Test
         - SHA-224 Known Answer Test
         - SHA-256 Known Answer Test
         - SHA-384 Known Answer Test
         - SHA-512 Known Answer Test
         - RSA Pairwise Consistency Test
         - RSA Encrypt/Decrypt Known Answer Test
         - DSA Pairwise Consistency Test
         - ECDSA Pairwise Consistency Test
         - ECDH Pairwise Consistency Test
         - DH Pairwise Consistency Test
         - FIPS 186-2 RNG Known Answer Test

   Firmware Integrity Test – 32-bit CRC

   B. Critical Functions Tests

      1. Memory Check – Walking 1’s test

   C. Conditional Self-Tests

1. Continuous Random Number Generator (RNG) test – performed on NDRNG and RNG
2. DSA Sign/Verify Pairwise Consistency Test
3. RSA Sign/Verify Pairwise Consistency Test
4. ECDSA Sign/Verify Pairwise Consistency Test
5. Diffie-Hellman Primitive Test
6. Firmware Load Test – RSA signature verification

6. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
7. Power-up self tests do not require any operator action.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
11. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
12. The module does not support a maintenance interface or role.
13. The module does not output intermediate key values.

The module is not configured to operate in FIPS-mode by default. The following steps must be taken to enable FIPS-mode operation:

1. Alter configuration encryption key from its default value.
2. Configure an Administrator account upon first access to the module.
3. Ensure minimum password length is at least 6 characters.
4. Ensure download of software updates without a digital signature is not allowed.
5. Disable Telnet access or make sure that Telnet is not enabled.
6. Configure the module (IPSEC, SSH v2, IKE v1, v2, SNMP (no security claimed)) to use only the Approved algorithms specified in Section 3 above.
7. Set “Forgotten Password Recovery” to disabled.

If any if these steps are omitted then a “FIPS L2 Mode” alarm will be generated. The Crypto-Officer must zeroize all keys when switching from the Approved FIPS mode of operation to the non-FIPS mode and vice versa.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip embedded module is production quality containing standard passivation. Module components are protected by a metal enclosure protected with tamper evident seals.

The module's enclosure is protected with 5 tamper evident seals. Please refer to Figures 3, 4 and 5 for the correct placement of the tamper evident seals.

Note: The tamper evident seals will be applied in manufacturing. If tamper evident seals need to be replaced, the module will have to be returned to the manufacturer.

Figure 3 - Label placement (Top)

Figure 4 - Label placement (Bottom, Rear, and Left)

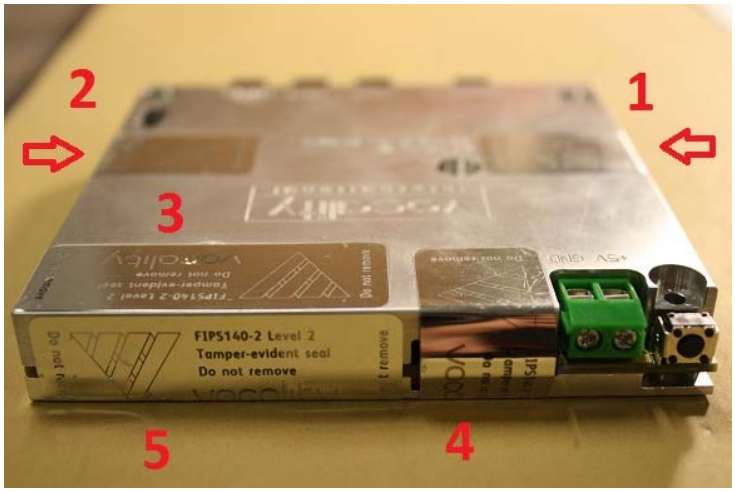

Figure 5 - Label placement (Top and Rear)

9.2 Operator Required Actions

Table 12 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test
Tamper Evident Seals	6 months

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

11 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

12 Definitions and Acronyms

AES - Advanced Encryption Standard
CO - Cryptographic Officer
CSP - Critical Security Parameter
DES - Data Encryption Standard
DH - Diffie-Hellman
DSA - Digital Signature Algorithm
ECDH - Elliptic Curve Diffie-Hellman
ECDSA - Elliptic Curve Digital Signature Algorithm
EMC - Electromagnetic Compatibility
EMI - Electromagnetic Interference
FIPS - Federal Information Processing Standard
HMAC - Keyed-Hash Message Authentication Code
RAM - Random Access Memory
RNG - Random Number Generator
RSA - Rivest, Shamir and Adleman Algorithm
SHA – Secure Hash Algorithm
TDES – Triple-DES