Ecutel Cryptographic Service Module

(Software Version 1.0)

FIPS 140-2 Non-Proprietary
Security Policy

Level 1 Validation
Version 0.11

September, 2006

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Ecutel Cryptographic Service Module (ECSM) version 1.0 from Ecutel Systems, Inc. This Security Policy describes how the Ecutel Cryptographic Service Module (ECSM) version 1.0 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 Ecutel Cryptographic Service Module version 1.0 is referred to in this document as the ECSM, the crypto module, the cryptographic module, the software module, or the module.

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 Ecutel Systems, Inc. website (http://www.ecutel.com) contains information on the full line of products from Ecutel Systems.

- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

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 Ecutel Systems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Ecutel Systems and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Ecutel Systems.

ECUTEL CRYPTOGRAPHIC SERVICE MODULE (ECSM) VERSION 1.0

Overview

Ecutel Systems is a pioneering provider of standards-based, secure enterprise mobility software. The company’s technology brings seamless mobility to all facets of the enterprise, from simple and secure access for mobile workers to remote management for IT professionals. Ecutel products empower users to become truly mobile professionals. Their system uniquely combines standards-based security and the IPSec and Mobile IP mobility protocols to enable users to roam in the office on wireless and wired Local Area Networks (LANs) or outside on public networks – all while maintaining their connection to the network resources back at the office. No matter where a user is working from, their productivity remains the same as if they were sitting at his desk in the office.

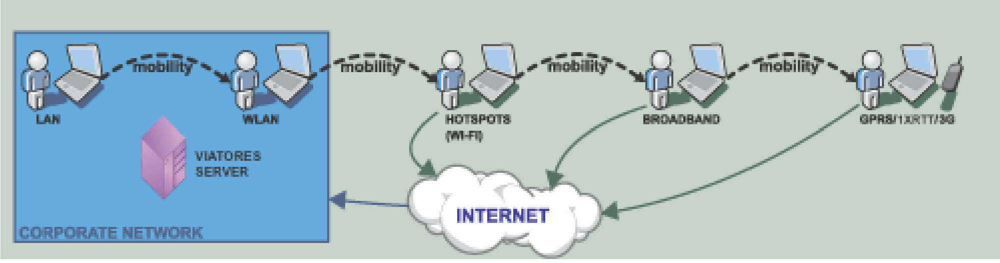

Figure 1 - Secure Seamless Session

The ECSM is the solution, exclusive to Ecutel system, to provide security and authenticity of the traffic data. The module is capable of encryption with the AES (FIPS 197) and TDES (FIPS 46-3) algorithms; and message authentication is implemented using HMAC SHA-1 (FIPS 198).

Module Specifications

The Ecutel Cryptographic Service Module (ECSM) is a cryptographic library that offers cryptographic functionalities to Ecutel products only. It is a library that is installed on a machine as a constituent of a host application. The ECSM is classified as a multi-chip standalone module that meets overall level 1 FIPS 140-2 requirements.

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	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level per FIPS 140-2 Section

The logical cryptographic boundary of the module is comprises the ECSM software running on Windows XP, Linux RedHat, or Windows Mobile for Pocket PC 2003 Operating Systems. The module is composed of a library file which is cross-compiled on the specified operating systems in both User- and Kernel-modes.

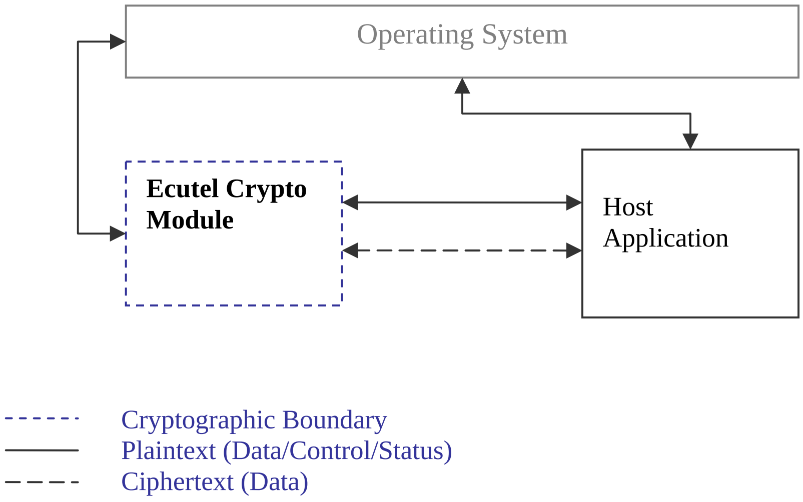

Figure 2 - Module Logical Block Diagram

The module is validated for use on a standard PC running the Windows XP, RedHat Linux, or on a Pocket PC running Windows Mobile for Pocket PC 2003 Operating Systems. The table below summarizes library forms running for different OS depending on mode.

Operating System	Mode	Library File Name
Windows XP	User	Ecucrypt.dll
	Kernel	Ecucrypt.sys
Windows Mobile for Pocket PC 2003	User and Kernel	Ecucrypt.dll
Linux RedHat Kernel 2.6	User	Ecucrypt.so
	Kernel	Ecucrypt.o

In addition to the binaries, the physical device consists of the motherboard circuits, the central processing unit (CPU), random access memory (RAM), read-only memory (ROM), and PC case, expansion cards, and other hardware components included in the PC such as hard disk, floppy disk, CD-ROM drive, power supply, and fans. The physical cryptographic boundary of the module is the hard, opaque metal and plastic enclosure of the PC or the Pocket PC. Physical block diagrams are shown below for the PC and the Pocket PC. Block diagram for standard PC is shown in Figure 3.

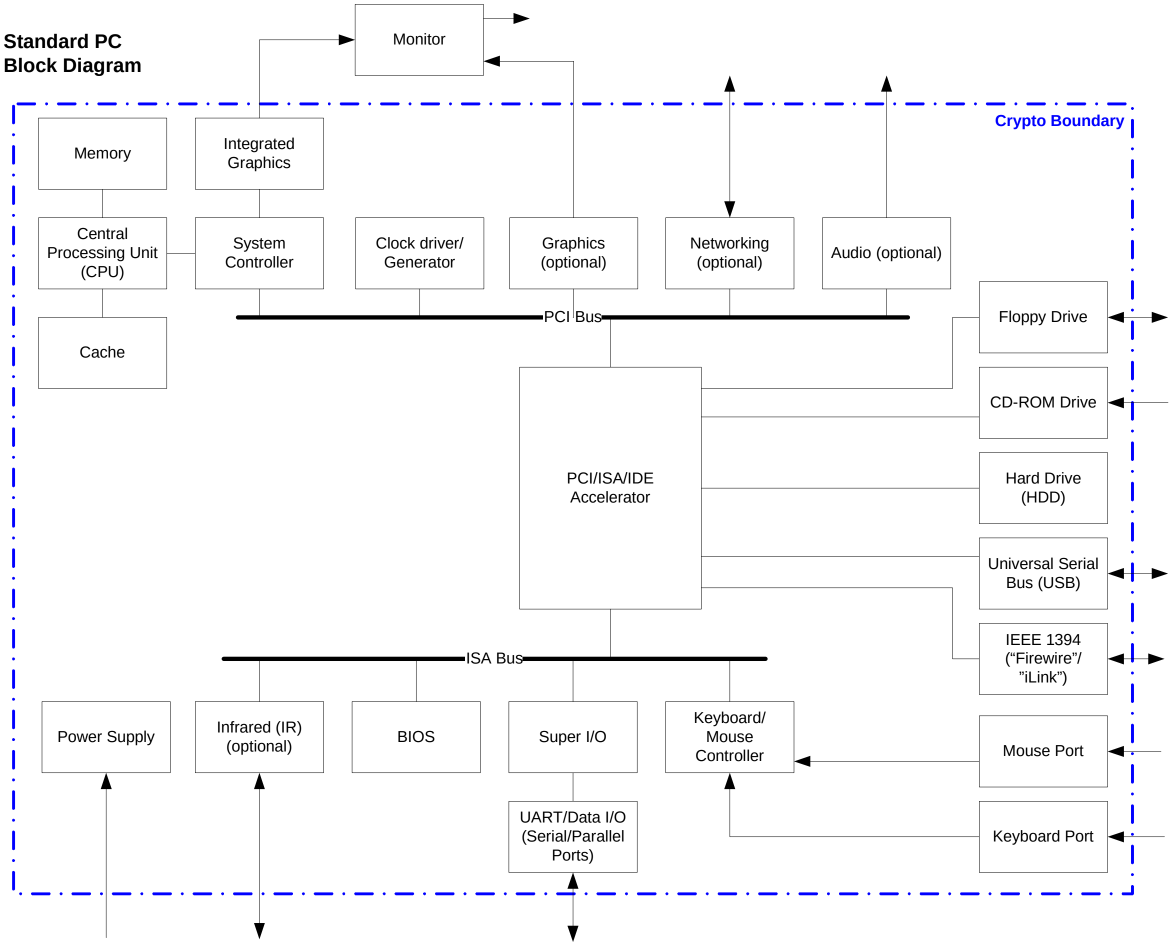

Figure 3 - Standard PC Physical Block Diagram

Figure 4 below shows the block diagram for a Pocket PC.

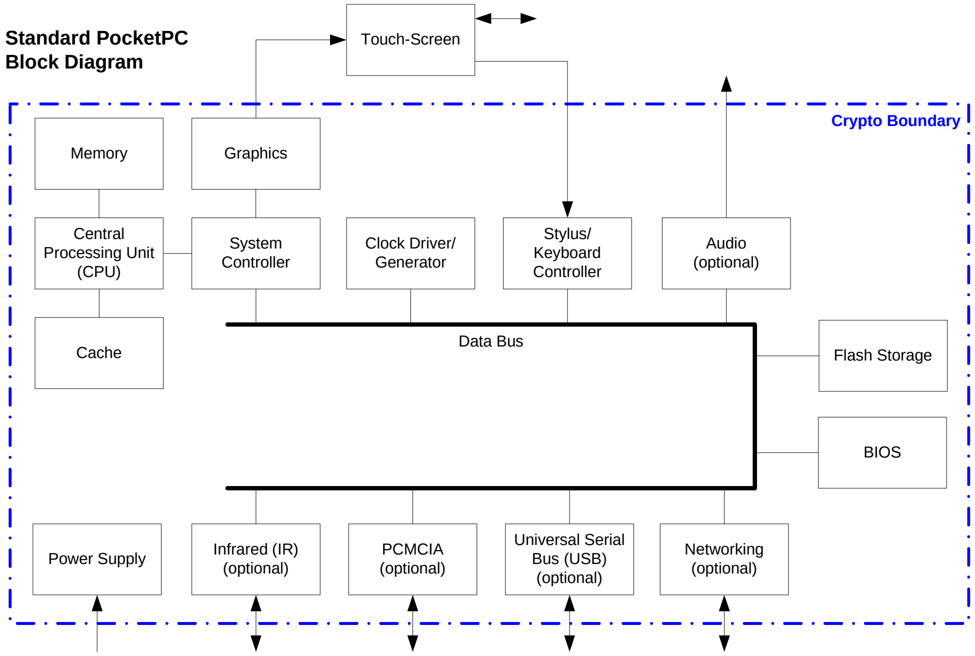

Figure 4 – Standard PocketPC Physical Block Diagram

Module Interfaces

The module's logical interfaces exist at a lower level in the software as APIs. Physically, ports and interfaces are considered to be those of the host PC and Pocket PC. Both the API and physical interfaces are mapped into logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Interface		**Module Logical Interface**	**FIPS 140-2 Logical Interface**
Standard PC	**Pocket PC**		
Keyboard, mouse, CD-ROM, floppy disk, and serial/USB/parallel/network ports	Touch screen and serial/USB/network ports	Function calls that accept, as their arguments, data to be used or processed by the module.	Data Input Interface
Hard Disk, floppy disk, monitor, and serial/USB/parallel/network ports	Touch screen and serial/USB/network ports	Arguments for a function that specify where the result of the function is stored.	Data Output Interface
Keyboard, CD-ROM, floppy disk, mouse, and serial/USB/parallel/network port	Touch screen and serial/USB/network ports	Function calls utilized to initiate the module and the function calls used to control the operation of the module.	Control Input Interface
Hard Disk, floppy disk, monitor, and serial/USB/parallel/network ports	Touch screen and serial/USB/network ports	Return values for function calls	Status Output Interface
Power Interface	Power Interface	Not Applicable	Power Interface

Table 2 – Physical Ports and Logical Interfaces

Roles and Services

The module supports two operator roles: “Crypto-Officer” and “User.” The module operator assumes either of the roles based on the services required. The module does not support operator authentication. Both of the roles and their responsibilities are described below.

Crypto-Officer Role

The Crypto-Officer (CO) is expected to install and configure the module. Once the module is running, the CO can perform all management, configuration and administration of the module. The Crypto-Officer is also responsible for monitoring the module’s configuration and operational status from the host application log files. Please see *Secure Operation* section for details.

The following table lists the Crypto-Officer role’s services:

Service	Description	Input	Output	CSP	Type of Access to CSP
Install	Install the module	Commands	Result of installation	None	--
Uninstall	Uninstall the module	Command	Module uninstalled	None	--
Monitor	Configure of the module	Command	Module setting	None	--
Run Self-Test	Perform the self-test on demand	Command	Status output	Integrity Check Key	Read
Terminate functionalities	Terminate module services by forced self-test failure	Command	module unloaded	Symmetric keys	Read

Table 3 – Crypto-Officer Services, Descriptions, and CSPs

User Role

The User role accesses the module’s cryptographic services that include encryption/decryption and authentication functionalities. The following table lists the User role’s services:

Service	Description	Input	Output	CSP	Type of Access to CSP
Symmetric Key Operation	AES or TDES encryption and decryption	API calls, symmetric key, initial value, input data	Encrypted or decrypted data, status output	TDES Key	Read/Write
				AES Key	Read/Write
Message Authentication	Generates HMAC value for a message	API calls, HMAC key, message	MAC value, Status output	HMAC key	Read/Write
Hashing Operation	Generate message digest using SHA-1	API calls, message	Message digest, status output	None	--
Random Number Generation	Provide seed and generate random number	API calls, seed value	Random number, status output	Seed	Read/Write

Table 4 – User Services, Descriptions, and CSPs

Physical Security

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 hardware platform is a standard PC or PocketPC which has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC Part 15.

Operational Environment

The module runs on the general purpose Windows XP, Windows Mobile for Pocket PC 2003, and RedHat Linux operating systems. RedHat Linux and Windows XP must be configured for single user mode per NIST CMVP guidance for FIPS 140-2 compliance. The module was tested on Windows XP, Linux RedHat Kernel version 2.6, and Windows Mobile for Pocket PC 2003. Single user mode configuration instructions for RedHat Linux and Windows XP can be found in the *Secure Operation* section.

Cryptographic Key Management

The module implements the following FIPS-approved software algorithms:

- AES (ECB, CBC) – FIPS 197 (certificate #381)
  Key sizes: 128 bits

- Triple DES (ECB, CBC) -1, 2, 3 keying option – FIPS 46-3 (certificate #425)
  Key sizes: 168 bits

- SHA-1 (Byte-oriented) – FIPS 180-2 (certificate #456)

- HMAC SHA-1 – FIPS 198 (certificate #170)
  Key sizes: 20 bytes
  MAC size: 20 bytes

- PRNG – ANSI X9.31 Appendix A.2.4 (certificate #183)

The module supports the following critical security parameters:

Key or CSP	**Key type**	**Generation**	**Storage**	**Use**
TDES Symmetric Key	3 key TDES keys	Generated externally. Entered in plaintext	Plaintext in volatile memory	Encrypt or decrypt traffic data
AES Symmetric Key	128 bit AES key	Generated externally. Entered in plaintext	Plaintext in volatile memory	Encrypt or decrypt traffic data
Authentication Key	20 byte HMAC key	Generated externally. Entered in plaintext	Plaintext in volatile memory	Generate MAC value to authenticate data

Key or CSP	Key type	Generation	Storage	Use
Integrity Check Key	20 byte HMAC key	Externally generated, hard coded in the module	Stored on hard-drive in module	Software integrity test
ANSI X9.31 PRNG seed	Seed value	Generated externally. Enter in plaintext	Plaintext in volatile memory	Generate pseudo random number

Table 5 – Listing of Critical Security Parameters

Access Control Policy

Crypto-Officer has read access to Integrity Check Key via *Run Self-Test* service (Table 3). User-role services (Table 4) have read access to these symmetric keys and the Authentication Key. While performing the cryptographic operations the API handles these key objects.

Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The module performs the following self-tests:

- Power-up Self-tests:
    - Software Integrity Test – Verifies the integrity of the software binaries of the module by using a HMAC SHA-1 MAC.
    - Cryptographic Algorithm Tests
        - AES KAT
        - Triple-DES KAT
        - HMAC SHA-1 KAT
        - SHA-1 KAT
        - ANSI X9.31 PRNG KAT
- Continuous Self-Tests:
    - Continuous Random Number Generator Tests for FIPS 140-2 Approved ANSI X9.31 Appendix A.2.4
    - Continuous Random Number Generator Tests for entropy gathering

Design Assurance

Ecutel utilizes Concurrent Versions System (CVS) as its version control system. This software provides access control, versioning, and logging.

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

Mitigation of Other Attacks

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

SECURE OPERATION

The module meets level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the FIPS-Approved mode of operation.

Crypto-Officer Guidance

The Crypto-Officer is responsible for installing/uninstalling, configuring, and managing the module. Before installing the module, the Crypto-Officer should make sure that the Operating System is in single user mode.

Operating System Setup

The Crypto Officer must maintain control of the installation media.

FIPS 140-2 mandates that a cryptographic module be limited to a single user at a time. Before the module can be installed, the Crypto Officer must have a standard PC running Windows XP configured for single user mode, RedHat Linux configured for single user mode, or a PocketPC running Windows Mobile[1].

To ensure that RedHat Linux is running in single user mode, the Crypto Officer must delete or disable all accounts except for the root account. Additionally, to ensure only one user can be logged in at a time, the root account must be configured to only allow console access logins and all remote server services must be disabled (e.g., telnet or rlogin server daemon).

The specific procedure to configure RedHat Linux System for single user mode is described below.

1. Login as the "root" user.

2. Edit the system files /etc/passwd and /etc/shadow and remove all the users except "root" and the pseudo-users. Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.

3. Edit the system file /etc/nsswitch.conf and make "files" the only option for "passwd", "group", and "shadow". This disables NIS and other name services for users and groups.

4. In the /etc/xinetd.d directory, edit the files "rexec", "rlogin", "rsh", "rsync", "telnet", and "wu-ftpd", and set the value of "disable" to "yes".

5. Reboot the system for the changes to take effect.

[1] Since Windows Mobile for Pocket PC 2003 is inherently a single user operating system, no special preparation procedures are required.

- More information can be found at: http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf

To configure Windows XP for single user mode, the CO must ensure that all remote guest accounts are disabled in order to ensure that only one human operator can log into the OS at a time. The services that need to be turned off for Windows XP are –

- Fast-user switching (irrelevant if PC is a domain member)
- Terminal services
- Remote registry service
- Secondary logon service
- Telnet service
- Remote desktop and remote assistance service

Once the Operating System has been properly configured, the Crypto Officer (system "root" account) can be used for installing/uninstalling software and administrating the module.

Initial Setup

The software module will be provided to the users by Ecutel System, Inc. for exclusive use in their products only. The module is installed during installation of the host application. The installation procedure is described in the products' manual.

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

Management

The Crypto-Officer should monitor the module's status by regularly checking the log information. Products' manual instructs how to check the log information. The cryptographic module offers FIPS 140-2 approved functions as specified in *Table 4*.

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.

ACRONYMS

Acronym	Definition
API	Application Programming Interface
CD-ROM	Compact Disc - Read-Only Memory
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CVS	Concurrent Versions System
ECSM	Ecutel Cryptographic Service Module
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash MAC
IR	InfraRed
IP	Internet Protocol
IPSec	IP Security
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institutes of Standards and Technology
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
ROM	Read-Only Memory
USB	Universal Serial Bus
VSS	Visual Source Safe
VPN	Virtual Private Network