FIPS 140-2 Security Policy

for

Motorola, Inc

Motorola Wireless Fusion on Windows Mobile Cryptographic Module

Hybrid Module

Software Component Version: 3.00

Hardware Component Version: CX 55222

Document Version Number: 0.98

1. Module Description

Motorola Wireless Fusion on Windows Mobile Cryptographic Module provides wireless data encryption functionality to devices running Windows Mobile operating system. These mobile computing devices are used for business process automation applications in a number of vertical markets such as retail, manufacturing and transportation.

For the purposes of FIPS 140-2 the module is classified as a software hybrid module. This hybrid module includes the following components:

- single-chip hardware component, part number CX 55222
- Jedi10 DLL software component to drive the hardware component

The hardware component consists of a single chip that is physically protected by a hard tamper-resistant epoxy layer. The physical boundary of the hardware component is the boundary of the epoxy layer.

The hybrid module is installed into a GPC, which typically has handheld dimensions and provides wireless functionality. Since the GPC where the module is installed is a multi-chip standalone device, the module is qualified as a multi-chip standalone module.

The main purpose of the module is to encrypt/decrypt data.

FIPS 140-2 conformance testing of the module was performed at Security Level 1. The following configurations were tested by the lab:

Software Component Version	**Operating Systems**	**Hardware Component Version**
JEDI10.dll Version 3.00	Windows Mobile 6.1 Windows Mobile 6.5	CX 55222

The following table summarizes FIPS 140-2 compliance claims

Security Requirements Section	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1

EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of other attacks	N/A

2. Cryptographic Boundary

The cryptographic boundary of the module includes the JEDI10.dll software binary (software component) as well as the hardware chip (hardware component).

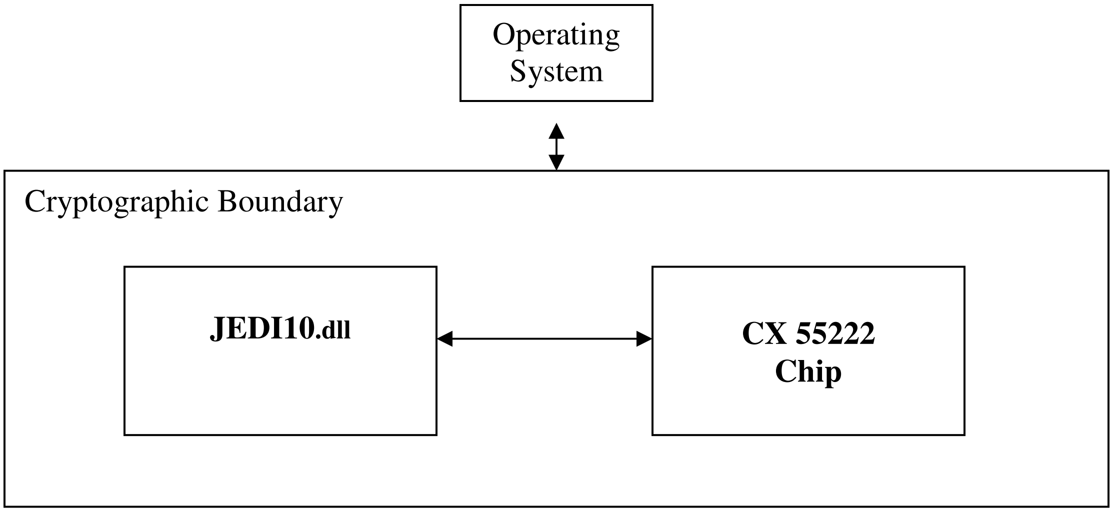
The module includes the following logical interfaces:

- Control Input Interface: software API commands and command parameters used to control and configure module operation. The Control Input Interface also includes the registry values used to control module behavior
- Status Output Interface: return values from software API commands used to obtain information on the status of the module. The Status Output Interface also includes the log file where the module messages are output
- Data Input Interface: data inputs to the software API commads
- Data Output Interface: data outputs of the software API commands

All module interfaces, inputs and outputs are provided by the software component.

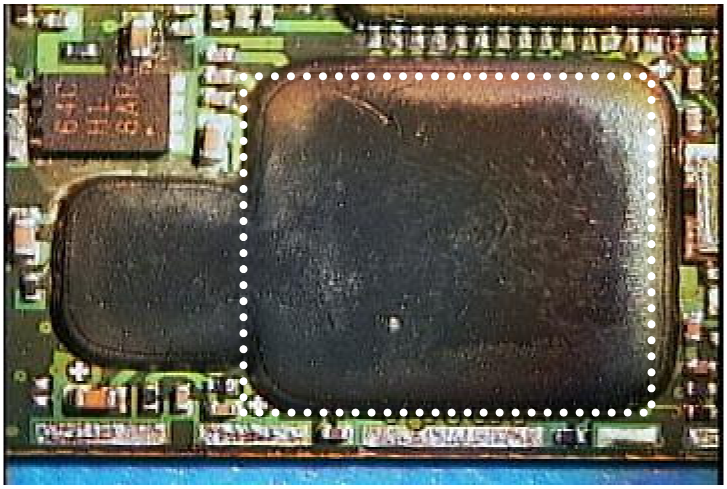
The block diagram for the module is provided below.

Figure 1. Block Diagram



An image of the hardware component protected by hard epoxy is provided below. The physical boundary of the hardware component is denoted by the dotted line in Figure 2. The hardware component is a single chip located under the coating indicated by the dotted line in Figure 2.

Figure 2. Hardware Component



3. Roles and Services

The module provides the following roles:

1. User.
2. Crypto Officer.

The Crypto Officer configures the module and manages its cryptographic functionality. The User employs the cryptographic services provided by the module.

The module provides the following services to the User and Crypto Officer.

Service	Role	Access to Cryptographic Keys and CSPs R- read or use W – write or generate, Z – zeroize N/A – no CSPs are accessed by this service
Run-self tests	Crypto Officer	N/A
Get status of the module	Crypto Officer	N/A
Set AES encryption key	Crypto Officer	W (sets AES encryption key)
Encrypt/decrypt wireless data using the AES encryption key	User	R (uses the AES encryption key to encrypt/decrypt wireless data)
Zeroize	Crypto Officer	Z (zeroizes the AES encryption key)

Note: the AES encryption key is the only cryptographic key used by the module other than the keys used for self-tests. The AES encryption key is zeroized by the key zeroization procedure.

Note: the AES encryption key is entered into the module using manual distribution. The operator of the handheld GPC will type in the key into the handheld GPC where the module is installed.

In the non-FIPS mode of operation the module provides the following non-compliant services: encrypt/decrypt wireless data using WEP and TKIP wireless standards. By policy, to stay in the FIPS-approved mode of operation, the operator shall not use WEP and TKIP.

4. Security Functions

The table below lists approved cryptographic algorithms employed by the module

Algorithm	Certificate #
AES	1036 and 1038
HMAC	582
SHS	989

In the non-Approved mode of operation the module implements the following non-Approved cryptographic algorithms: TKIP, RC4.

5. Key Management

The following cryptographic keys are supported by the module

Name and Type	Generation or establishment	Usage
AES encryption key	Set by the application using the module’s software API	Encryption of the wireless data
HMAC SHA-1 integrity key	Pre-set in the module binary	Used to check integrity of the module at power-on

All keys are stored inside the module in plaintext. The module does not provide a functionality to output cryptographic keys. The AES encryption key can be input using the module’s software API. The AES encryption key is entered into the module using manual distribution. The operator of the handheld device will type in the key into the handheld device, where the module is installed. The GUI application will then input the key into the module in plaintext.

To zeroize the keys inside the logical cryptographic boundary one shall power down the GPC, which will also power down the module. Since all keys stored in the module are stored in the volatile memory, powering down the module destroys the keys.

6. Self Tests.

The module runs a set of self-tests on power-up. If one of the self-tests fails, the module transitions into an error state where all data output and cryptographic operations are disabled. The self-test success or error message is output into the log file.

The module runs self-tests for the following algorithms

Algorithm	Test
AES	Known Answer Test (encrypt/decrypt)
SHA-1	Tested during the integrity check
HMAC SHA-1	Tested during the integrity check

7. Approved Mode of Operation

The approved mode of operation is enabled by the Crypto Officer role.

The module is installed as follows:

1. Copy the JEDI10.dll and JEDI10.dtr files into the “Windows” folder.
2. Set the registry value
HKEY_LOCAL_MACHINE\Comm\Jedi10_1\Parms\FipsModeKey
to be nonzero.
3. Power-cycle the module.

Whenever the software has been reloaded the FIPS mode self tests are performed. If these tests are successful, then the module is operational in the FIPS Mode. If they are not successful, then the module is disabled.

The FIPS mode is defined by policy. In particular, to stay in the FIPS mode, the user shall avoid using the following services that use non-approved crypto algorithms: encrypt/decrypt wireless data using WEP and TKIP wireless standards.