FIPS 140-2 Security Policy

TEL_crypto_module

v1.1.0, v1.1.1

FIPS 140-2 Level 1 Validation

Vendor:	Tait Ltd
Document Version:	2.6
Version Date:	18 April 2013

Table of Contents

1. Introduction

This document specifies the non-proprietary *Security Policy* for the TEL_crypto_module. It is provided as part of the validation for the Crypto Module to level 1 of Federal Information Processing Standard (FIPS) 140-2. Two versions of Crypto Module are described in this version of the Security Policy.

Crypto Module v1.1.0 supports the following physical configurations:
Texas Instruments TMS320C5509 DSP
Texas Instruments TMS320C5510 DSP

Crypto Module v1.1.1 supports the following physical configurations:
Texas Instruments TMS320C5505A DSP
Texas Instruments TMS320C5505M1 DSP

2. Module Specification

The TEL_crypto_module is a compiled and versioned linkable library, running on the TMS320C55xx Digital Signal Processors (DSP) as listed in the Introduction. Henceforth, the library package of the TEL_crypto_module will simply be referred to as the "module".

2.1. Module

For the purposes of FIPS 140-2 validation, the Crypto Module is a *firmware, single-chip module*. The module is provided as a compiled linkable library running on the Texas Instruments TMS320C55xx DSP. Only the linkable library provided by the vendor is considered as a module for the FIPS 140-2 validation process.

The module contains FIPS 140-2 *approved cryptographic algorithms*, and for historic reasons also contains a non-compliant implementation of RNG. The module is only capable of operating in a FIPS 140-2 mode of operation.

Clients use the Application Programming Interface (API) provided (see Services, Section 4.2) to access these functions.

The module provides real-time voice and data encryption for radio communications equipment (Portable Terminals, Mobile Terminals or Base Stations).

Any changes to the Crypto Module firmware will invalidate FIPS 140-2 certification.

2.2. Boundaries

The firmware module that comprises the Crypto Module defines the *logical boundary* for the module.

The *physical boundary* for v1.1.0 of the module is one of:

- the Texas Instruments TMS320C5509 DSP
- the Texas Instruments TMS320C5510 DSP

The *physical boundary* for v1.1.1 of the module is one of:

- the Texas Instruments TMS320C5505A DSP
- the Texas Instruments TMS320C5505M1 DSP

2.3. Hardware Platform

The v1.1.0 of the Crypto Module is used on the 9100 series of Tait digital radio products. This includes the TB9100 Base Station, the TM9100 Mobile Terminal range, and the TP9100 Portable Terminal range. The physical boundary of the TM9100 and the TP9100 is common (TMS320C5509 DSP).

For FIPS 140-2 testing, v1.1.0 of the module was installed and tested on the following Texas Instruments DSP devices:

TMS320C5509 DSP, hosted on a Tait TP9100 Portable Terminal
TMS320C5510 DSP, hosted on a Tait TB9100 Base Station

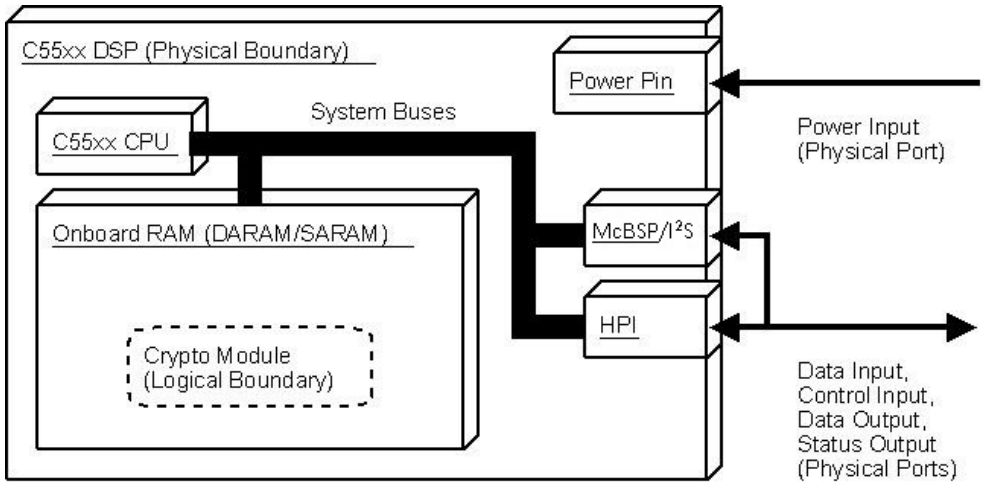
The v1.1.1 of the Crypto Module is used on the 9300 and 9400 series of Tait digital radio Terminal products. This includes the TM9300 Mobile Terminal range, the TP9300 Portable Terminal range, the TM9400 Mobile Terminal range and the TP9400 Portable Terminal range. The physical boundaries of the 9300 and 9400 series of Terminals are common and can be either the TMS320C5505A DSP or the TMS320C5505M1 DSP.

For FIPS 140-2 testing, v1.1.1 of the module was installed and tested on the following Texas Instruments DSP devices:

TMS320C5505A DSP, hosted on a Tait TP9300 Portable Terminal
TMS320C5505M1 DSP, hosted on a Tait TP9400 Portable Terminal

2.4. Module Block Diagram

The following block diagram shows the specifications of the module, with the McBSP/I^2S (Multi-Channel Buffered Serial Port/Integrated Inter-chip Sound), HPI/EHPI (Host Port Interface/Enhanced Host Port Interface), as physical input and output ports.



3. Module Ports and Interfaces

Since the crypto module is a linkable firmware library, logical interfaces are specified. The logical interface is in the form of a firmware Application Program Interface. The logical interface is specified as follows:

Data Input Interface: The parameters that are supplied in the function call are the data inputs.

Data Output Interface: Parameters in function calls that hold output values are defined as the data output interface.

Control Input Interface: API calls exported by the module are the control input interface.

Status Output Interface: Return values from function calls are the status output interface.

FIPS 140-2 Interface	Module Logical Interface	Module Physical Port
Data Input	Data passed to API calls to be used by the module	McBSP/I^2S, HPI
Data Output	Data returned from API calls, generated by the module	McBSP/I^2S, HPI
Control Input	API calls exported by the module	McBSP/I^2S, HPI
Status Output	API function returns	McBSP/I^2S, HPI
Power	N/A	Power pin

All logical interfaces share the same physical ports. Information from different interface categories is kept separate through the semantics of arguments to function calls to the crypto module API. Arguments to and return values from function calls are designated as input, output, status or control.

4. Roles, Services and Authentication

This section of the Security Policy defines the services that can be run and the security relevant data that be accessed when the module is used by clients in specific roles.

4.1. Roles

The module supports two roles as defined by FIPS 140-2:

1. **User**

   The User is any entity that can access the services provided by the module. It is implicitly selected when API calls are made to the module.

2. **Crypto Officer**

   The Crypto Officer is any entity that can access the services provided by the module, install the module onto the hardware platform, or configure the calling client. It is implicitly selected when installing the module or configuring the operating environment. The Crypto Officer is also responsible for key entry into the radio equipment (Portable Terminal, Mobile Terminal or Base Station).

The module does not support a *Maintenance role* or a bypass capability.

4.2. Services

The module provides the FIPS 140-2 approved services described in this section.

Service	Algorithm/ Module Version: Cert #	FIPS	Services	Role
Symmetric Block Cipher	Triple-DES (3-key) / v1.1.0: #539, v1.1.1: #1462	FIPS 46-3	crypto_ProcessDataEcb (Triple-DES, 192) crypto_ProcessDataCbc (Triple-DES, 192) crypto_ProcessDataOfb (Triple-DES, 192)	User/Crypto Officer
	AES (128-bit key) / v1.1.0: #537, v1.1.1: #2328	FIPS 197	crypto_ProcessDataEcb (AES, 128) crypto_ProcessDataCbc (AES, 128) crypto_ProcessDataOfb (AES, 128)	User/Crypto Officer
	AES (256-bit key) / v1.1.0: #537, v1.1.1: #2328	FIPS 197	crypto_ProcessDataEcb (AES, 256) crypto_ProcessDataCbc (AES, 256) crypto_ProcessDataOfb (AES, 256)	User/Crypto Officer
Hash algorithm	SHA1 / v1.1.0: #672, v1.1.1: #2012	FIPS 180-1	crypto_Sha1Init crypto_Sha1Update crypto_Sha1Final	User/Crypto Officer
Keyed-hash message authentication code	HMAC-SHA1 / v1.1.0: #327, v1.1.1: #1443	FIPS 198	crypto_HmacSha1	User/Crypto Officer
Random Number Generator (RNG)[1]	ANSI X9.31-1998 - Appendix A / v1.1.0: #343, v1.1.1: Non-compliant	N/A	crypto_Rng	User/Crypto Officer
Other	Module Status	N/A	crypto_GetModuleStatus	User/Crypto Officer
	Module Initialisation (including Power On Self Test)	N/A	crypto_Init	Crypto Officer

[1] The RNG function in v1.1.1 of the Crypto Module is classified as a non-compliant algorithm, and should not be executed by clients of the crypto module.

	Module Lockdown	N/A	crypto_LockDown	User/Crypto Officer
	Symmetric Block Cipher Initialisation	N/A	crypto_InitCipher	User/Crypto Officer
	Symmetric Block Cipher set IV	N/A	crypto_SetIv	User/Crypto Officer
	Power On Self Test	N/A	crypto_Init	Crypto Officer
	Key Zeroization	N/A	crypto_InitCipher	User/Crypto Officer

The Critical Security Parameters (CSPs) for each type of service are shown below.

Service	**CSPs**	**Client Access Rights (R and/or W)**
Symmetric Block Cipher	Secret key	RW (the secret key belongs to the client; the module is simply given a pointer to the key stored in RAM by the client)
Random Number Generator (compliant in v1.1.0; non-compliant in v1.1.1)	Private Seed Public Seed Random Number	Private Seed (V) – None Public Seed (Date/Time) – RW Random Number – R
Self Test Integrity check using HMAC-SHA-1	Secret key	None

4.3. Authentication

For the purposes of FIPS 140-2 level 1, the Module does not implement user authentication; it depends on the operating environment and hardware for user authentication.

5. Physical Security

All TMS320C55xx series chips are production grade components that have standard passivation and meet the FIPS 140-2 level 1 requirements for physical security. The crypto module is a single chip firmware implementation with version identification. The module versions were certified for and tested on the following DSP hardware configurations:

v1.1.0: the TMS320C5509 and the TMS320C5510

v1.1.1: the TMS320C5505A and the TMS320C5505M1

6. Operational Environment

6.1. Operating Environment Requirements

The module is completely independent of the rest of the code running on the DSP. All memory used by the module is either within the module boundaries in memory or provided as a pointer by the calling client – memory is not dynamically allocated by the module. It does not communicate with any external processes, so the module cannot accidentally disclose CSPs.

The module is restricted to a single user mode of operation. The operating environment is responsible for multi-tasking operations so that other processes cannot intervene when the module is active at a particular instance in time.

6.2. Module Integrity

The integrity of the FIPS 140-2 validated firmware module is verified as part of the Power-On Self-Test (POST) at runtime using an approved integrity technique (HMAC-SHA-1).

7. Cryptographic Key Management

The calling client provides and is responsible for the cryptographic keys used by the module. The client is responsible for any key storage on persistent media. The module is only given a pointer to the plaintext key meta data in RAM – key meta data are not stored in any way by the module itself. The key meta data are only stored within RAM, referenced by a pointer within the crypto module, which points to memory outside of the crypto module. The key meta data remain in RAM for all subsequent calls to be used in functions providing cryptographic services.

The module does not provide any key generation, key storage or key establishment services.

The RNG can be used to generate random numbers for the client. There is no internal coupling within the crypto module boundary between the RNG and other approved algorithms. The output of the RNG may be used by clients to generate an IV to initialize the approved cryptographic algorithms. Note however, that the RNG implementation is considered a non-compliant algorithm in v1.1.1 of the Crypto Module.

Key zeroization may be performed by power cycling the DSP. Data output is inhibited during zeroization since the Crypto Module cannot execute when no power is applied to the DSP.

8. Self-Tests

The module implements a POST and Conditional tests for the RNG to ensure the correct operation of approved cryptographic algorithms and security functions. To exit any error states after a KAT or Integrity test has failed, the crypto module must be power-cycled. Data output is inhibited while the Crypto Module is in the POST state.

8.1. Power On Self-Test

The module starts up in an uninitialized state, and must be initialized by the Crypto Officer before any approved cryptographic algorithms and security functions can be used. As part of the initialisation routine, a POST is executed to ensure the integrity of the module and the correct operation of its security services. If the POST fails, the module is returned to the uninitialized state, so that approved cryptographic algorithms and security functions cannot be performed.

8.1.1 Cryptographic Algorithm Test

Known Answer Tests (KATs) are performed for:

- Triple-DES, AES-128, and AES-256. For each algorithm, critical functions for all algorithm operation modes (ECB, CBC, OFB) are tested as well. Two blocks of known plain and cipher text values are compared with intermediate test values in each case to test whether the algorithms perform in the correct manner for multi-block messages.
- SHA-1 (only used as part of the HMAC-SHA-1 integrity test, with no user interface). The KAT compares known input data and hash with intermediate values.
- HMAC-SHA-1 (only used as part of the integrity test, with no user interface). The KAT compares known input data and hash generated using a known key with intermediate values.
- RNG. The KAT sets all seeds to known values and compares the output to the known value.

8.1.2 Integrity Test

The read-only data section of the module contains an HMAC-SHA-1 key and Message Authentication Code (MAC) value, written at build time. A MAC is calculated by running HMAC-SHA-1 over the read-only data and code sections of the module in memory (excluding the stored MAC value). During the integrity test, this MAC value is calculated and compared with the stored MAC to check for modifications to the binary code.

8.1.3 On Demand Self-Test

The POST can be run again on demand by reinitializing the module using the crypto_Init() function call or by power-cycling the module.

8.2. Conditional Tests

The module also implements ongoing tests during execution. If a conditional test fails, the module enters the Error state and transitions into the Uninitialized state, so that approved cryptographic algorithms and security functions cannot be performed.

8.2.1 Continuous Random Number Generator Test

The module implements a continuous random number generator test, running each time the RNG is invoked[2]. As part of the test, the previously stored 64-bit random number is stored as a variable in RAM (not persistent media). During the test, the previously stored 64-bit random number is compared with the generated 64-bit random number. If they are identical, the test fails, and the module enters the Error state and transitions into the Uninitialized state, so that approved cryptographic algorithms and security functions cannot be performed. When the RNG is invoked for the first time, it stores rather than outputting the first random number it generates. A second random number is generated and output after running the continuous random number generator test.

[2] The RNG function in v1.1.1 of the Crypto Module is classified as a non-compliant algorithm, and should not be executed by clients of the crypto module.

9. Mitigation of Other Attacks

The module does not provide additional mechanisms to mitigate attacks beyond those required by FIPS 140-2 as part of the firmware integrity check.

10. Design Assurance

10.1. Configuration Management

The vendor ensures the integrity of the module during development by using the secure configuration management system Subversion (SVN). The SVN repository stores each distinct model of the module's source code, as well as the binary deliverable. The repository is hosted by an Apache HTTP server, and is protected using Apache's own authentication system. Only approved users can access the module files within the repository.

Each time a new version of a file is stored in the repository, it is automatically given a unique SVN revision number. These revision numbers are used internally to allow developers to roll back to previous versions of the module if necessary, and are not seen by end users.

Each release of the deliverable binary has an associated Crypto Module version number. This number is stored within the crypto_Api.h header file as a string, "CRYPTO_VERSION M.m.b", where M.m.b is the unique version number. The version number uses a conventional numbering scheme, i.e. the first digit for major releases, the second digit for minor revisions and the third digit for developers to track build releases.

10.2. Delivery and Operation

See documents *Crypto Module APIs and Notes* and the *Crypto Officer Guide* for details regarding the correct procedure for module installation and configuration.

10.3. Secure Operation

Users should ensure that keys are not disclosed to unauthorised users.

For Base Stations, ssh access should be disabled or a secure password, changed regularly, should be used.

Unauthorized users should not have physical access to Base Stations or Terminals for any length of time.

10.4. Guidance Documents

The *Crypto Officer Guide* document provides information to Crypto Officers about the correct procedure for installing and configuring the module. The document *Crypto Module APIs and Notes* explains to the developer the proper usage of the modules Approved Services. The *User Guide* explains to the user the proper usage of the modules Approved Services.

Appendix A: Master Components List

A.1.Hardware Components

The Texas Instruments DSPs listed in the Introduction are the only hardware element of the Crypto Module. It is a standard production grade integrated circuit designed to meet commercial grade operating specifications. The hardware elements are not part of the FIPS 140-2 validation for the module.

A.2.Firmware Components

The only firmware component is the Crypto Module.

Two versions of the Crypto Module are specified in this Security Policy, namely v1.1.0 and v1.1.1.