FIPS 140-2 Security Policy for

Marvell Semiconductor, Inc.

Armada Mobile Processor

Hardware Version: Armada PXA-2128[1] and
Armada PXA-610[2]

Firmware Version: 2128-1.1[1] and 610-1.1[2]

Document Version: 1.6

1. Module Description

The ARMADA™ mobile processor (models PXA-2128 and PXA-610), also referred to as the Module within this document, is a Marvell's System-on-Chip (SoC) product that is designed for mainstream Mobile Internet Devices (MIDs), connected consumer products, e-readers, smart phones, media players and new personal information appliances. It delivers the best combination of fast, PC-caliber processing, an uncompromised Internet experience, and full 1080p HD quality video and 3D graphics — all in the lightweight form factors with extended battery life that consumers want.

The PXA-2128 and PXA-610 SoCs are equipped with a dedicated security hardware module known as WTM (Wireless Trusted Module) that offers the trusted computing services required for user authentication, identity management, secure storage as well as secure communication. Within WTM, there is a pool of the hardware cryptographic engines that performs at high throughput of the cryptographic operations over a set of FIPS-Approved algorithms, such as AES, TDES, SHA, HMAC, RSA, and EC-DSA. In addition, the on-chip hardware entropy-bit-generator under WTM is a reliable source of the entropy seeding to the FIPS-Approved DRBG schemes. The dedicated WTM secure firmware is responsible for device trusted boot, access control, authentication, and key management.

The threat model for the device empowered by the PXA-2128 (and PXA-610) covers the case of the stolen device that is powered down. The confidentiality of the information and data within secure storage of the stolen device must be maintained even if the disk (or FLASH) is removed and attempts are made to recover the data directly from the media. The PXA-2128 (and PXA-610) addresses this problem by wrapping the data with device RKEK based key management hierarchy. The thief of the stolen device is also blocked to access the privileged services since the respective critical sensitive information is under the protection of the secure storage.

The PXA-2128 (and PXA-610) is designed to meet requirements of FIPS 140-2 at Security Level 3. The trusted computing and cryptographic boundary of the SoC corresponds to the physical boundary of the chip packaging. Physical ports of the SoC are comprised by hardware pins. The module is covered with a hard opaque tamper-evident material. The hardness testing was performed at ambient temperature.

During the manufacturing process the module is configured to only support the Approved Mode of Operation. To indicate the Approved Mode of Operation, the module writes the value corresponding to the Approved mode of operation to external memory.

The test platform integrating PXA-2128 or PXA-610 SoC is the reference design. PXA-2128 or PXA-610 could be potentially integrated into a system level product (e.g. the mobile phone, or other consumer electronic appliances) by Marvell's customers targeted for production; however such configuration were not tested during the FIPS 140-2 testing process.

Figure 1. A photograph of the Armada PXA-2128

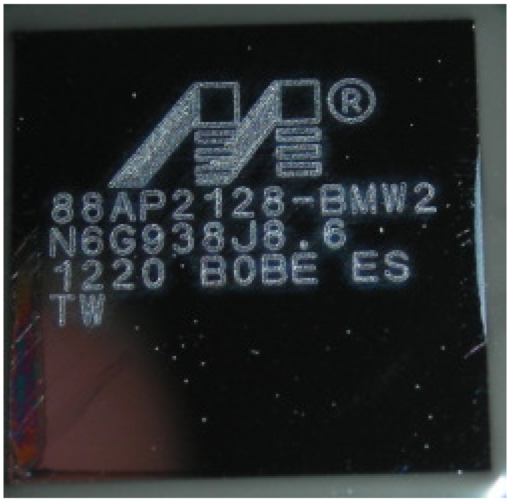
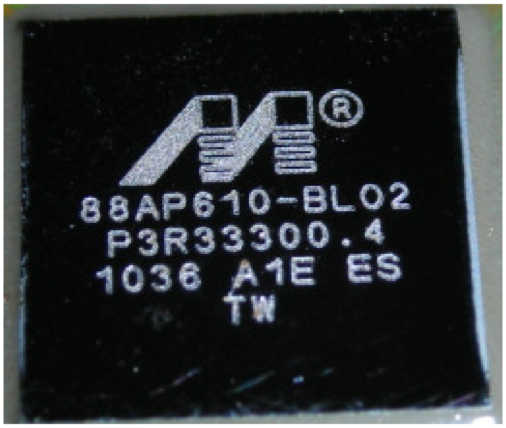


Figure 2. A photograph of the Armada PXA-610



The Module’s Security Level Statement is presented in the table below.

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

2. Roles, Services and Authentication

The module provides the following roles: Crypto Officer and User.

The Crypto Officer configures the module and manages its cryptographic functionality.

The User utilizes cryptographic functionality provided by the module.

The table below provides information about authentication mechanisms employed by each role.

Role	Type of Authentication	Authentication credentials and Identity
Crypto Officer	Identity-based authentication	224-bit password along with 32-bit user ID are used to authenticate the user to import or export the endorsement key to/from the device. The password and user ID are also used to authenticate the user to enroll the OEM Digital Rights Management /Device Management (DRM/DM) Keys (either private or symmetric) into the module. The DRM/DM Keys that are transmitted to the module as a part of the enrollment process are protected using AES encryption. The 224-bit password along with 32-bit user ID are used to authenticate the user to allow generation of a user key. 256-bit digest is used to authenticate the erasure of the keys stored in the secure on-chip OTP storage media (zeroization). RSA or ECDSA public key and PIN are used to authenticate the firmware loading.

Role	Type of Authentication	Authentication credentials and Identity
User	Identity-based authentication	224-bit password along with 32-bit user ID are used to authenticate the user to activate the use of the DRM/DM key by loading the key into the respective cryptographic engine. 224-bit password along with 32-bit user ID are used to authenticate the user to activate the use of the previously generated user key by loading the key into the respective cryptographic engine. 224-bit password along with 32-bit user ID are used to authenticate the user to activate the use of the public key by loading the key into the respective cryptographic engine.

The module provides the following services.

Service	Role	Access to Cryptographic Keys and CSPs R – read or use W – Write or Generate Z – zeroize
AES encryption/ decryption	User	AES Keys: R
TDES encryption/ decryption	User	TDES Keys: R
HMAC generation	User	HMAC Keys: R
Digital signature signing and verifying using RSA	User	RSA Key Pair: R
Digital signature signing and verifying using EC-DSA	User	EC-DSA Key Pair: R
Using non-approved, but allowed EC-DH to generate shared key	User	EC-DH Shared Key: W
Run Self Tests	Crypto Officer User	N/A
Reset to factory defaults/Zeroize Keys and CSPs	Crypto Officer	CO’s password: R All Keys and CSPs: Z
Symmetric or asymmetric key generation	Crypto Officer	RKEK: R SKEK: R Endorsement Key: R CO’s password: R

Service	**Role**	**Access to Cryptographic Keys and CSPs** **R – read or use** **W – Write or Generate** **Z – zeroize**
		Newly generated Key: W User's password: W
Enrollment of private or symmetric DRM/DM keys.	Crypto Officer	Transit Key: R RKEK: R SKEK: R CO's password: R User's password: W Newly enrolled key: W
Public key activation	User	Requested public key: W User's password: R
Firmware load	Crypto Officer	PKCS/EC-DSA public Key: R PIN: R
Get status of the module	Crypto Officer User	N/A
Key Import and Export	Crypto Officer	RKEK: R SKEK: R CO's password: R Respective Imported key: W Respective Exported key: R
Key Activation	User	Requested Key: R User's Password: R

3. Security Functions

The table below lists approved cryptographic algorithms implemented by the module:

Algorithm	Certificate #
AES(ECB/CBC/CTR/XTS) – Key size(128/192/256)	1982 and 2133
TDES (ECB/CBC)	1285 and 1357
SHA(SHA-1/224/256/384/512)	1737 and 1857
HMAC(HMAC-SHA-1/224/256/384/512)	1195 and 1303
RSA (PKCS#1v1.5-Sig(gen/ver))[1]	1028 and 1102
ECDSA (Sig(gen/ver)/PKG/PKV)[2]	287 and 323
DRBG (SP800-90 Hash Based – SHA-1/224/256/384/512)	182 and 238

The table below lists non-Approved, but allowed cryptographic algorithms employed by the module

Algorithm	Usage
EC-DH	Implements support for EC-DH key agreement algorithm for use by client software
AES (Certs. #1982 and #2133, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)	Protection of keys

4. Key Management

The following cryptographic keys are supported by the module:

Name and Type	Generation or establishment	Algorithm	Usage
RKEK	Created at the factory	AES	Used to encrypt SKEKs

[1] The module does not support 1024-bit keys or SHA-1 for Digital Signature Generation
[2] The module does not support SHA-1 for Digital Signature Generation

Name and Type	**Generation or establishment**	**Algorithm**	**Usage**
SKEKs	Created at the factory or generated after deployment	AES	Used to encrypt Endorsement keys and user keys
Transit Keys	Created at the factory	AES	Used to encrypt private or secret DRM/DM keys during their enrollment.
Endorsement Keys	Created at factory	AES	Used to encrypt userid/password of the user of newly generated keys
AES user keys	Generated by the module or imported into the module or derived through EC-DH	AES	Used by user
TDES user keys	Generated by the module or imported into the module or derived through EC-DH	TDES	Used by user
HMAC user keys	Generated by the module or imported into the module or derived through EC-DH	HMAC	Used by user
RSA user keys	Generated by the module or imported into the module	RSA	Used by user
ECDSA user keys	Generated by the module or imported into the module	ECDSA	Used by user

Name and Type	Generation or establishment	Algorithm	Usage
EC-DH user keys	Generated by the module	EC-DH	Used by user

All keys, except for RKEK and Transit Keys, can be imported into/exported from the module.

5. Self-Tests

The module runs power-on self-tests (POST) for the following algorithms:

Algorithm	Test
AES	Known Answer Test (Encrypt/Decrypt)
TDES	Known Answer Test (Encrypt/Decrypt)
HMAC	Known Answer Test
SHS	Covered by HMAC Test
DRBG	Known Answer Test
RSA	Known Answer Test (Sign KAT/Verify KAT)
EC-DSA	Known Answer Test

The module implements the power-on digital signature (using PKCS#1v1.5 and EC-DSA) check over the firmware image at firmware loading, and it implements the continuous DRBG test for SP800-90. The module also performs the continuous test at runtime over the entropy that is used to seed the DRBG.

A pair-wise consistency test is performed whenever the module creates an asymmetric public/private key pair for use by RSA or ECDSA. The module will complete a sign/verify operation on every generated key pair to ensure that key generation is functioning properly. If the operation fails, an error is reported and the key pair is discarded.

6. Crypto Officer Guidance

6.1 Secure Setup Instructions

The following steps shall be performed by the Crypto Officer to perform the initial setup of the product:

1. Generate User Keys and SKEKs as needed
2. Export the newly generated keys as needed
3. Enroll DRM/DM keys as needed
4. Export the newly enrolled DRM/DM keys as needed

6.2 Secure Operation

The following rules shall be followed by the Crypto Officer to achieve secure operation of the module:

In case the module needs to be discarded, perform key zeroization, by issuing the WTM_OTP_KEY_ERASURE command followed by the power cycle, before discarding the module.

7. User Guidance

7.1 Secure Operation

The following rules shall be followed by the User to achieve secure operation of the module:

Generate a strong, non-dictionary based 224-bit password. Output of a FIPS-Approved random number generator can be used to create highly secure passwords.

8. Physical Security

The module consists of production-grade components that are covered with a hard opaque tamper-evident material to deter direct observation, probing, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module. The material is opaque within the visible spectrum. The material completely covers the module and deters direct observation, probing, or manipulation of the module.