Relocation Management Software

VERN™ RMW Crypto Library

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Relocation
Management
Worldwide

Relocation Management Worldwide, Inc.
http://www.relocationmw.com
1-(866)-815-8300

Version History

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Description of Change
	Robert G	9/1/2014	*Bob B*	9/2/2014	*Initial Draft*
1.0	*Robert G*	11/22/2014	*Rob G*	11/22/2014	*Submitted Versioned SVN*
1.1	*Robert G*	4/10/2015	*Rob G*	4/12/2015	*COACT Feedback*
1.2	*Robert G*	9/1/2015	*Rob G*	9/14/2015	*COACT Feedback*
1.3	*Robert G*	12/29/2015	*Rob G*	12/29/2015	*Minor Changes*
1.4	*Robert G*	1/15/2016	*Rob G*	1/15/2016	*Minor Changes*

1 Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1 Identification

Module Name	VERN™ RMW Crypto Library
Software Module Version	1.2

1.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the VERN™ RMW Crypto Library, also referred to as "the module" within this document. This Security Policy details the secure operation of VERN™ Cryptographic Module as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.3 References

For more information on VERN™ products please visit: http://www.relocationmw.com. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be VERN™ proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact VERN™.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

TERM	DESCRIPTION
AES	Advanced Encryption Standard
CBC	Operation mode referred to as Cipher Block Chaining
KS	Key Size
API	Application Programming Interface
FIPS	Federal Information Processing Standard
OS	Operating System
SHA	Secure Hash Algorithm
RAM	Random-access Memory
IDisposable	Interface Dispose Method
HMAC	Keyed-hash Message Authentication Code

Figure 1 Document terminology

2 VERN™ RMW Crypto Library

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

The module provides cryptographic services to VERN™ products.

The module is packaged differently depending on its operational environment.

2.2 Module Specification

The VERN™ RMW Crypto Library is a software library that provides cryptographic services to VERN™ products. The module provides FIPS 140-2 validated cryptographic algorithms for services such as Encrypt, Decrypt and Hash. The module does not directly implement any of these protocols. Instead it provides applications with a library interface that enables them to access the various cryptographic algorithm functions supplied by the module. The consuming applications can then use these functions to implement the various protocols. There are no unapproved modes of operation.

2.2.1 Hardware, Software and Firmware components

There are no specific hardware or firmware requirements for the module. The module is a software-only module which resides on either a General-Purpose Computer or proprietary hardware (see Figure 3).

It is packaged as one distinct binary image, one for each of the following operating environments:

File Name	Operating Environment	Version	Processor
rmwVERNCryptoLib.dll	Microsoft® Windows® Server 2012 (Single-User Mode)	1.2	Intel Xeon E5410 Quad Core Processor

Figure 2 Module Binary Image

2.2.2 Cryptographic Boundary

The cryptographic boundary of the module is the case of the platform on which it is installed. See Figure 3. The module is a software module running in a defined operating environment on a general-purpose computer or other hardware platform. The processor of this platform executes all software. All software components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

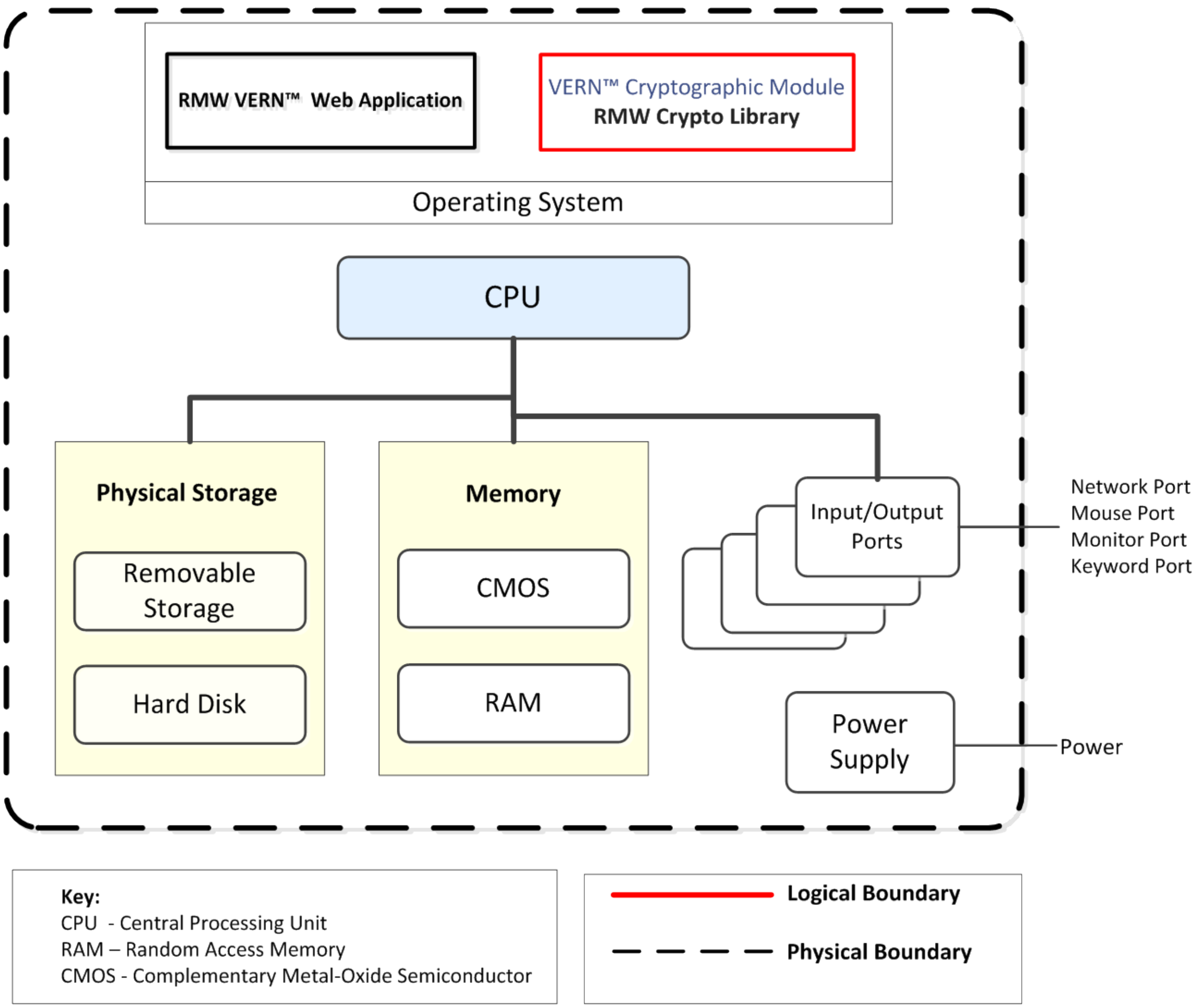

Figure 3 Block Diagram of the Cryptographic Boundary

2.2.3 Scope of Evaluation

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

SECURITY REQUIREMENTS SECTION	LEVEL
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 4 Security Level Specifications per Individual Areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

Approved algorithms

The following table provides details of the approved algorithms that are included within the module:

Algorithm Type	Algorithm	Status	Certificate Number	Notes
Hashing	SHA-256 SHS (FIPS 180-4)	Approved	**#2713**	SHA-256 (BYTE-only)
Symmetric key	AES (CBC 256) AES (FIPS 197)	Approved	**#3275**	CBC (e/d; 256)
HMAC	HMAC-SHA256 (FIPS 198-1)	Approved	**#2240**	SHA-256 (Key Size Ranges Tested: KS=BS)

Figure 5 Approved Algorithms

There are no unapproved modes of operation.

2.2.5 Components excluded from the security requirements of the standard

There are no components excluded from the security requirements of the standard.

2.3 Physical ports and logical interfaces

The module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the device on which it is installed. The device shall run a supported operating system (OS) and supporting sufficient interfaces to allow operators to initiate cryptographic operations and determine the module status.

The module provides its logical interfaces via Application Programming Interface (API) calls. This logical interface exposes services (described in section 2.4.2) that applications utilize directly.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 Logical Interface	Module Mapping	Physical Interface
Data Input	Parameters passed to the module via API calls	Network Port Input, Mouse/Keyboard Port Input
Data Output	Data returned from the module via API calls	Network Port Output, Monitor Port Output
Control Input	API Calls and/or parameters passed to API calls	
Status Output	Information received in response to API calls	Network Port Input, Monitor Port Output
Power Interface	There is no separate power or maintenance access interface beyond the power interface provided by the device the contains that module	

Figure 6 Module Interfaces

2.4 Roles, Services and Authentication

2.4.1 Roles

The RMW Crypto Library implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Section 2.4.2 summarizes the services available to each role.

ROLE	DESCRIPTION
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Figure 7 Roles

2.4.2 Services

Most of the services provided by the module are provided via access to API calls using interfaces exposed by the module.

However, some of the services, such as power-up module integrity testing are performed automatically and so have no function API, but do provide status output.

The keys are not persistently stored. The API service methods listed that utilize an input below are wrapped in internal IDisposable class member method which explicitly releases resources. This provides key zerorization after the completion of a service.

SERVICE	ROLE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION	ACCESS TO CSPS
AesCryptoProvider.Encrypt	User	Plaintext data	Encrypted data	Performs AES encryption. Service includes IDisposable interface that automatically releases the utilized resources on service completion.	Access to Data Key Crypto Officer – None User - RWU
AesCryptoProvider.Decrypt	User	Encrypted data	Plaintext data	Performs AES decryption. Service includes IDisposable interface that automatically releases the utilized resources on service completion.	Access to Data Key Crypto Officer – None User - RWU
SHACryptoProvider.GenerateHash	User	Data	Hash of data	Performs SHA Hash. Service includes IDisposable interface that automatically releases the utilized resources on service completion.	No access to CSPs Crypto Officer – None User - None
Show Status	Crypto Officer	Status request	Module status.	Status is returned in response to individual service API calls; and at the completion of the self-tests.	No access to CSPs Crypto Officer – None User - None
Self-tests	Crypto Officer	None	Success/Failure	Self-tests run automatically at power up.	Access to Data Key and HMAC Key Crypto Officer – U User - None
Installation	Crypto Officer	None	Installed module	The module is deployed as part of a VERN™ product installation.	Access to Data Key and HMAC Key Crypto Officer – U User - None
Uninstallation	Crypto Officer	None	Uninstalled module	The module is uninstalled during the uninstallation of the product that deployed the module.	Access to Data Key and HMAC Key Crypto Officer – U User - None

SERVICE	ROLE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION	ACCESS TO CSPS
Key Zeroization	Crypto Officer	None	Module keys removed	Uninstall runs service to remove known answer test keys used in module.	Access to Data Key and HMAC Key Crypto Officer – W User - None

R = Read W = Write U = Use

Figure 8 Services

Note: Key zeroization zeroes all keys and CSPs; this is a "write" operation in that all keys are overwritten using internal class IDisposable member method and resources are released.

2.4.3 Authentication

The module has been evaluated at FIPS 140-2 level 1 and no claims are made for authentication.

2.5 Physical Security

The RMW Crypto Library is a software-only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

2.6 Operational Environment

The RMW Crypto Library has been tested on and found to be conformant with the requirements of FIPS 140-2 overall Level 1 on the following platforms:

PLATFORM	CPU	OPERATING SYSTEM (ALL TESTED IN SINGLE-USER MODE
Dell Power Edge 2950	Intel (Xeon 2.33GHz) x 2	Windows Server 2012 Standard (Single-User Mode)

Figure 9 Operating Platforms

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

The module is also capable of running on the following platforms but has not been tested during this evaluation and no compliance is being claimed on these platforms:

- Windows 7 with SP1
- Windows 8
- Windows Server 2008 R2

Requires Microsoft® .Net Framework 4.0 and greater

The cryptographic module runs in the thread context of the calling application. This provides it with protection from all other processes, preventing access to all keys, intermediate key generation values, and other CSPs.

The task scheduler and architecture of the operational environment maintain the integrity of the cryptographic module.

The module supports only one single user and only one operator can have access to the device that contains the module at a time.

The GPC(s) used during testing are assumed to have met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.7 Cryptographic Key Management

2.7.1 Key Generation

The module does not generate any keys.

2.7.2 Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

KEY	
Key Name	AesCryptoProvider Data Key

Purpose	To encrypt and decrypt data using the symmetric encryption services.
Length/Strength	AES 256 bit
Generation/Establishment	Externally generated
Storage Location	Not persistently stored. Process uses protected RAM and parameters operated in separated thread process.
Keys Supplied Encrypted or Plaintext	Plaintext
Entry/Output	Plaintext
Destruction	Zerorized using internal IDisposable member method

KEY	
Key Name	HMAC Key
Purpose	Key secret used in combination generate message hash for integrity self-test.
Length/Strength	256 bit
Generation/Establishment	Externally generated
Storage Location	Not persistently stored. Process uses protected RAM and parameters operated in separated thread process.
Keys Supplied Encrypted or Plaintext	Plaintext
Entry/Output	Plaintext
Destruction	Zerorized using internal IDisposable member method

Figure 10 Key Table

2.7.3 Key Destruction

All key material managed by the modules internal IDisposable class member method which explicitly releases resources. This provides key zerorization automatically after the operation has completes.

In this way all key material and CSPs are zeroized. There are no user-accessible plaintext keys or CSPs in the module.

2.8 Self-Tests

The module implements both power-up and self-tests as required by FIPS 140-2. The following section outlines the tests that are performed. When the power-up occurs, the operating system initializes the default entry point in the module which will run the self-tests listed below. If any of the below test below fail, this will cause the module to become inoperable and all services to become unavailable.

2.8.1 Power-up self-tests

OBJECT	TEST
Module Software	HMAC SHA-256 Integrity Check
SHA-256	Known answer test
AES-256	Known answer test

Figure 12 Power-up self-tests

2.9 Design Assurance

VERN™ employ industry standard best practices in the design, development, production and maintenance of all of its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this RMW Crypto Library Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

Delivery of the RMW Crypto Library to customers from the vendor is via the internet. When a customer purchases a license to use the RMW Crypto Library software, they are issued with a grant number as part of the sales process. This is then used as a password to allow them to download the software that they have purchased. The delivery channel is protected using secured sockets. Once the Crypto-Officer has downloaded the cryptographic module, it is his responsibility to ensure its secure delivery to the users that he is responsible for.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks

3.0 Secure Operation

3.1 Initial Setup

3.1.1 Enable FIPS Mode Compliance

The operational environment requires running under Microsoft® Windows® FIPS mode enabled. This is a critical operational setting for the module to run. The module will not operate and return an error message if this setting is off or not available. A Crypto-Officer will need to confirm Microsoft® Windows® FIPS mode by verifying in the registry of the system the below entry is set to **“1” or ON** using the Microsoft® Windows® Registry software.

Navigate to the path below in registry to enable FIPS flag key DWORD “Enabled” to “1”.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy

3.1.2 Install Software

Run the VERN Crypto Installer software as a Crypto-Officer role on the server.

3.2 Crypto-Officer Guidance

The Crypto-Officer can initiate the execution of self-tests and can access the modules’ status reporting capability. Self-tests can be initiated at any time by power cycling the modules.

3.2.1 Management

It is the responsibility of the Crypto-Officer to ensure that the modules are set up to run securely. Please refer to Section 3.2 for guidance that the Crypto-Officer must follow for the modules to be considered in a FIPS-Approved mode of operation. Additionally, the Crypto-Officers should be careful to protect any secret/private keys in their possession.

3.2.2 Status Monitoring

Error message and status review is the responsibility of the Crypto-Officer. When any of the modules’ self-tests fail, the module reports an error message which can be viewed in the Crypto-Officer Web Administration portal, Windows Events Log and also available in the RMW Crypto Library specified log file path.

3.2.3 Zeroization

Keys entered to a service entry point are zeroized at the completion of the service explicitly calling IDisposable.

To completely destruct keys in the module, the following procedure below must be completed.

- Uninstalling the RMW Crypto Library from the server.
- Server platform hard drive or permanent storage media must be reformatted and overwritten at least once.