IPsec NULL Crypto Driver User Guide

Version 1.00

For use with IPsec NULL Crypto Driver module versions 1.02 and above

Exported on 06/13/2018

Table of Contents

1 System Overview

This chapter contains the fundamental information for this module.

The component sections are as follows:

- Introduction – describes the main elements of the module.
- Feature Check – summarizes the main features of the module as bullet points.
- Packages and Documents – the *Packages* section lists the packages that you need in order to use this module. The *Documents* section lists the relevant user guides.
- Change History – lists the earlier versions of this manual, giving the software version that each manual describes.

1.1 Introduction

This guide is for those who want to integrate HCC's NULL Crypto driver for IPsec so that IPsec can be used with either a NULL encryption suite or a NULL integrity check algorithm. This module is part of the CryptoCore™ Base security suite.

This driver is used in the following cases when either the encryption algorithm or the hash (integrity check) algorithm are not used:

- Because only one of the two algorithms (encryption or hashing) is required. In this case this module provides stub functions for the null algorithm.
- For testing.
- For debug.

You register the module with HCC's Embedded Encryption Manager (EEM), making it usable by other applications (for example, HCC's TLS/DTLS) through a standard interface. The EEM is the core component of HCC's encryption system.

This driver is used by IPsec to map NULL drivers to the existing encryption/authorization system.

- Null encryption (function **ipsec_null_enc_init_fn()**) copies input data to the output.
- Null hashing (function **ipsec_null_int_init_fn()**) generates a 0 length output buffer.

A complete test suite is included for validating the driver.

Note:

- Although every attempt has been made to simplify the system's use, to get the best results you must understand clearly the requirements of the systems you design.
- HCC Embedded offers hardware and firmware development consultancy to help you implement your system; contact sales@hcc-embedded.com.

1.2 Feature Check

The main features of the IPsec NULL module are the following:

- Conforms to the HCC Advanced Embedded Framework.
- Conforms to the HCC Coding Standard including full MISRA compliance.
- Designed for integration with both RTOS and non-RTOS based systems.
- Conforms to the HCC Embedded Encryption Manager (EEM) standard and is compatible with the EEM.
- Integral test suite gives complete logical coverage test of the driver.

1.3 Packages and Documents

Packages

The table below lists the packages that you need in order to use this module.

Package	Description
hcc_base_docs	This contains the two guides that will help you get started.
enc_base	The EEM base package.
enc_ipsec_null	The IPsec NULL Crypto Driver package described in this document.

Documents

For an overview of HCC verifiable embedded network encryption, see Product Information on the main HCC website.

Readers should note the points in the HCC Documentation Guidelines on the HCC documentation website.

HCC Firmware Quick Start Guide

This document describes how to install packages provided by HCC in the target development environment. Also follow the *Quick Start Guide* when HCC provides package updates.

HCC Source Tree Guide

This document describes the HCC source tree. It gives an overview of the system to make clear the logic behind its organization.

HCC Embedded Encryption Manager User Guide

This document describes the EEM.

HCC IPsec NULL Crypto Driver User Guide

This is this document.

1.4 Change History

To view or download manuals, see Encryption PDFs.

For the history of changes made to the package code itself, see History: enc_ipsec_null.

The current version of this manual is 1.00. The full list of versions is as follows:

Manual version	Date	Software version	Reason for change
1.00	2018-06-13	1.02	First online version.

2 Source File List

This section describes all the source code files included in the system. These files follow the HCC Embedded standard source tree system, described in the *HCC Source Tree Guide*. All references to file pathnames refer to locations within this standard source tree, not within the package you initially receive.

> **Note:** Do not modify any files except the configuration file.

2.1 API Header File

The file **src/api/api_enc_sw_ipsec_null.h** should be included by any application using the system. This is the only file that should be included by an application using this module. For details of the functions, see Application Programming Interface.

2.2 Configuration File

The file **src/config/config_enc_sw_ipsec_null.h** contains the configurable parameters of the system. Configure these as required. This is the only file in the module that you should modify.

2.3 System File

The file **src/enc/software/ipsec_null/ipsec_null.c** contains the source code. **This file should only be modified by HCC**.

2.4 Test File

The file **src/enc/test/test_ipsec_null.c** contains the test source code. **This file should only be modified by HCC**.

2.5 Version File

The file **src/version/ver_enc_sw_ipsec_null.h** contains the version number of this module. This version number is checked by all modules that use this module to ensure system consistency over upgrades.

3 Configuration Options

Set the system configuration options in the file **src/config/config_enc_sw_ipsec_null.h**. This section lists the available options and their default values.

IPSEC_NULL_TEST_ENABLE

Keep the default of 1 to enable the IPsec NULL test suite. Otherwise, set this to 0.

The following options set the IPsec NULL tests' init functions; redefine these if you want to use another set of drivers for a compatibility check.

IPSEC_NULL_TEST_IPSEC_NULL_ENC_INITFN

The IPsec NULL encryption driver init function. The default is `&ipsec_null_enc_init_fn`.

IPSEC_NULL_TEST_IPSEC_NULL_INT_INITFN

The IPsec NULL integrity check driver init function. The default is `&ipsec_null_int_init_fn`.

4 Application Programming Interface

This section describes the Application Programming Interface (API) functions and the error codes.

4.1 Functions

The functions are the following:

Function	Description
ipsec_null_enc_init_fn()	Called from the EEM, this registers the IPsec NULL encryption algorithm with it.
ipsec_null_int_init_fn()	Called from the EEM, this registers the IPsec NULL integrity check driver with it.
ipsec_null_register_tests()	Registers the IPsec NULL tests with the EEM test module.

ipsec_null_enc_init_fn

Call this initialization function from the EEM to register the IPsec NULL encryption algorithm with it. This call copies input data to the output.

This forwards the *t_enc_driver_fn* structure containing IPsec NULL functions to the EEM.
The *t_enc_driver_fn* structure is described in the the HCC Embedded Encryption Manager User Guide.

Format

```
t_enc_ret ipsec_null_enc_init_fn ( t_enc_driver_fn const * * const pp_encdriver )
```

Arguments

Parameter	Description	Type
pp_encdriver	A pointer to a *t_enc_driver_fn* structure containing IPsec NULL encryption functions.	t_enc_driver_fn * *

Return Values

Return value	Description
ENC_SUCCESS	Successful execution.
ENC_INVALID_ERR	The module has already been initialized.

ipsec_null_int_init_fn

Call this initialization function from the EEM to register the IPsec NULL integrity check driver with it. This call generates a 0 length output buffer.

This forwards the *t_enc_driver_fn* structure containing IPsec NULL integrity check driver functions to the EEM. The *t_enc_driver_fn* structure is described in the the HCC Embedded Encryption Manager User Guide.

Format

```
t_enc_ret ipsec_null_int_init_fn ( t_enc_driver_fn const * * const pp_encdriver )
```

Arguments

Parameter	Description	Type
pp_encdriver	A pointer to a *t_enc_driver_fn* structure containing IPsec NULL integrity check driver functions.	t_enc_driver_fn * *

Return Values

Return value	Description
ENC_SUCCESS	Successful execution.
ENC_INVALID_ERR	The module has already been initialized.

ipsec_null_register_tests

Call this function to register the IPsec NULL tests with the EEM test module.

> **Note:** The IPSEC_NULL_TEST_ENABLE configuration option must be set to 1 to enable this function.

Format

```
t_enc_ret ipsec_null_register_tests ( void )
```

Arguments

None.

Return Values

Return value	Description
ENC_SUCCESS	Successful execution.
Else	See Error Codes.

4.2 Error Codes

The table below lists the error codes that may be generated by the API calls.

Error code	Value	Meaning
ENC_SUCCESS	0	Successful execution.
ENC_INVALID_ERR	1	The module has already been initialized.

4.3 Defines

This following elements are defined in the API file:

Element	Value	Description
IPSEC_NULL_ENC_INIVECT_SIZE	0	NULL encryption init vector size.
IPSEC_NULL_ENC_KEY_LEN	0	NULL encryption key length.
IPSEC_NULL_ENC_BLOCK_SIZE	0	NULL encryption block size
IPSEC_NULL_INT_BLOCK_SIZE	0	NULL Integrity block size.
IPSEC_NULL_INT_ICV_SIZE	0	NULL Integrity check vector size.
IPSEC_NULL_INT_KEY_LEN	0	NULL Integrity key length.

5 Integration

The module is designed to be as open and as portable as possible. No assumptions are made about the functionality, the behavior, or even the existence, of the underlying operating system. For the system to work at its best, perform the porting outlined below. This is a straightforward task for an experienced engineer.

5.1 PSP Porting

The Platform Support Package (PSP) is designed to hold all platform-specific functionality, either because it relies on specific features of a target system, or because this provides the most efficient or flexible solution for the developer. For full details of these elements, see the *HCC Base Platform Support Package User Guide*.

The module makes use of the following standard PSP function:

Function	Package	Element	Description
psp_memcpy()	psp_base	psp_string	Copies a block of memory. The result is a binary copy of the data.