RSA Signature Algorithm User Guide

Version 1.20 BETA

For use with RSA module versions 2.0 and above

Date: 10-Jan-2017 11:04

Table of Contents

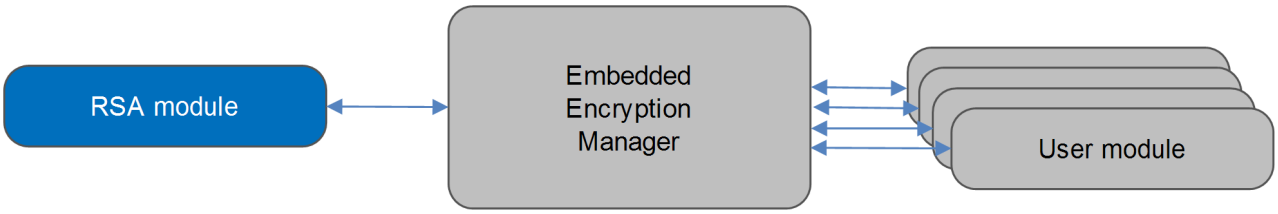
1 System Overview

1.1 Introduction

This guide is for those who want to implement encryption using the Rivest, Shamir and Adelman (RSA) signature algorithm. The RSA algorithm is most often used for public/private key encryption and decryption. Typically data is sent after it has been encrypted using the public key of the intended receiver, but can only be decrypted using the private key of the receiver.

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

The system structure is shown below:



RSA accepts two types of key format (ASN.1):

- A modulus and exponent value
- A private key with CRT data as specified in RFC 2437.

In the second case there are nine elements:

- The version (0).
- The modulus.
- The public exponent.
- The private exponent.
- Prime 1.
- Prime 2.
- Exponent 1.
- Exponent 2.
- A coefficient.

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 RSA 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.
- Supports a maximum key length of 4096 bits (512 bytes).
- Supports the RSA CRT algorithm (see RFC 2437 section 5.2.1).
- Can be verified by using the HCC Encryption Test Suite.

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_rsa	The RSA 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 Big Number Arithmetic Library API Specification

This document describes the big number arithmetic functions, some of which are used by this module.

HCC RSA Signature Algorithm User Guide

This is this document.

1.4 Change History

This section includes recent changes to this product. For a list of all the changes, refer to the file **src/history /enc/enc_rsa.txt** in the distribution package.

Version	Changes
2.0	Added New RSA padding type that can be configured by cypher data.
1.11	Corrected output buffer length checking.
1.10	Added the RSA CRT algorithm. This is used when a key with CRT data is provided.
1.09	Corrected parsing of RSA key. Compilation error is now raised when RSA_MAX_PUB_KEY_LEN has an invalid value.
1.08	Moved macro RSA_MAX_PUB_KEY_LEN to configuration file, so user can define maximum size of RSA key.
1.07	Added OID defines for RSA with SHA, RSA with SHA-256. Removed mutex clearing during initialization; this could cause compile error on OS.

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_rsa.h** is the only file that should be included by an application using this module. It defines the rsa_init_fn() function.

2.2 Configuration File

The file **src/config/config_enc_sw_rsa.h** contains the configurable system parameters. 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/rsa/rsa.c** is the source code file. **This file should only be modified by HCC**.

2.4 Version File

The file **src/version/ver_enc_sw_rsa.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_rsa.h**.

RSA_INSTANCE_NR

The maximum number of RSA driver instances. The default is 1.

RSA_MAX_PUB_KEY_LEN

The maximum RSA public key length in bytes. This must be less than or equal to the maximum length of a supported big number value (SBN_BUF_LEN in the base package's **config_enc.h** file). The default is 256 bytes.

> **Note:** The RSA strength is usually quoted in bits but this option uses bytes. The default of 256 bytes is 2048 bits.

4 Application Programming Interface

This section describes the single Application Programming Interface (API) function, the key lengths, and the error codes.

4.1 rsa_init_fn

Call this function from the EEM to forward the structure containing RSA functions to it.

Format

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

Arguments

Parameter	Description	Type
pp_encdriver	A pointer to a structure containing RSA functions.	t_enc_driver_fn * *

Return Values

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

4.2 Key Lengths

The key lengths are defined in the file **src/api/api_enc_sw_rsa.h**.

Name	Value	Description
RSA_MIN_PUB_KEY_LEN	64	The minimum public key length in bytes.
RSA_MAX_PUB_KEY_LEN	256	The maximum public key length in bytes.

4.3 Error Codes

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

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

4.4 Padding Types

The padding types are defined in the file **src/api/api_enc_sw_rsa.h**.

Name	Value	Description
RSA_PADDING_RANDOM	0	The signature padding is a pseudorandom value.
RSA_PADDING_SET	1	The signature padding is filled with 0xFF values.
RSA_PADDING_CLEAR	2	The signature padding is filled with 0x00 values.

5 Integration

The RSA 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 OS Abstraction Layer

The module uses the OS Abstraction Layer (OAL) that allows it to run seamlessly with a wide variety of RTOSes, or without an RTOS.

The module uses the following OAL components:

OAL Resource	Number Required
Tasks	0
Mutexes	1
Events	0

5.2 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 functions:

Function	Package	Element	Description
psp_memcpy()	psp_base	psp_string	Copies a block of memory. The result is a binary copy of the data.
psp_memset()	psp_base	psp_string	Sets the specified area of memory to the defined value.
PSP_WR_8BITARRAY_OFFSET()	psp_base	psp_array32	

The module uses the following big number arithmetic functions from the Big Number Arithmetic Library API.

Note: To improve performance, you can replace these functions with optimized or hardware-supported versions. For details, see the *HCC Big Number Arithmetic Library API Specification*.

Function	Description
bn_compare()	Compares two large numbers.
bn_get_be_buf()	Exports a big number to a big-endian buffer.
bn_get_power_modulo()	Calculates *p_a* raised to the power of *p_e*, modulo *p_m*, and stores the result in *p_r*.