Realtek rtl8195a crypto engine

Introduction here..

Contents

1 Introduction

This document illustrates how to use polarssl with crypto engine.

2 Crypto Engine

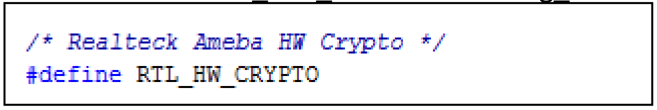
2.1 Main feature

Crypto engine is the hardware which can help CPU to do the encryption, decryption and authentication.

2.2 How to enable crypto engine

To enable hardware crypto engine, we have to change the configuration

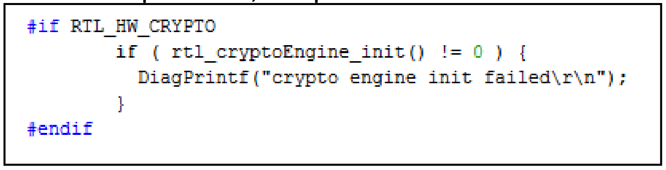
Enable #define RTL_HW_CRYPTO in config_rsa.h



```
/* Realteck Ameba HW Crypto */
#define RTL_HW_CRYPTO
```

Before crypto engine start to work, it needs initialization.

In the sample code, we put it in main.c



```
#if RTL_HW_CRYPTO
        if ( rtl_cryptoEngine_init() != 0 ) {
          DiagPrintf("crypto engine init failed\r\n");
        }
#endif
```

2.3 Crypto engine ssl feature

2.3.1 Authentication

The authentications that crypto engine supported are md5, sha1 and sha2.

Advantage and disadvantage between authentication with software and hardware:

Software:

Advantage: need less memory space compared with hardware

Disadvantage: need CPU to do the calculation

Hardware:

Advantage: Crypto engine help to process the calculation

Disadvantage: Need extra memory space to store different step’s result

After comparing the advantage and disadvantage, it suggests keep using software authentication.

2.3.2 Encryption and Decryption

The encryption and decryption that crypto engine supported are AES (cbc, ecb, ctr) DES (cbc, ecb) 3DES (cbc, ecb).

Now the polarssl supported ciphersuite is either CBC or GCM (GCM only when AES is enabled)

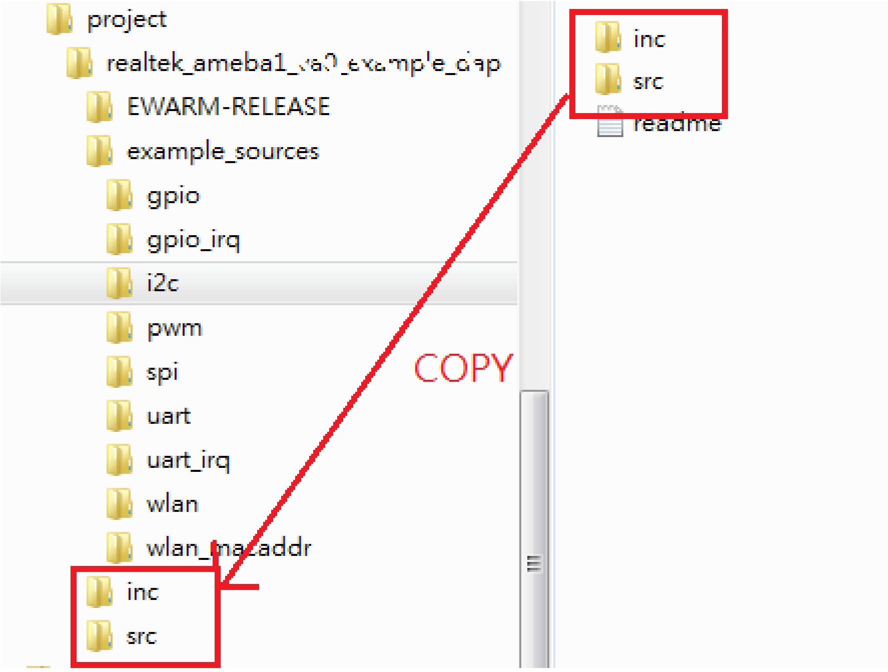
So that in the real ssl connect condition, it will choose CBC to be the encryption and decryption method. User can base on their own requirement and add new ciphersuite with others method.

2.4 How to use crypto engine with polarssl

User can refer to section 2.2 to enable hardware crypto engine. When it is doing ssl connect, during the handshake process it will choose the ciphersuite base on client and server. If the crypto method is within crypto engine supported, it will use crypto engine to process accordingly. Otherwise it will use software method to process.

3 How to use sample code to test crypto engine

To use sample crypto engine code, you can copy “src” and “inc” from project\project name\example sources\crypto engine\


project
realtek_ameba1_va0_example_dap
EWARM-RELEASE
example_sources
gpio
gpio_irq
i2c
pwm
spi
uart
uart_irq
wlan
wlan_macaddr
inc
src
COPY
inc
src
readme