CCA – COMPETENCE CENTRE

HTL Anichstraße

noindent

DIC-serial_crypto

Fabio Plunser

19. Februar 2021

Inhaltsverzeichnis

Abbildungsverzeichnis

Code

1 Aufgabenstellung

Die Aufgabe ist einfach (formuliert), implementieren Sie in Zephyr RTOS einen Krypto Prozessor der allen in test.py durchgeführten Tests erfolgreich absolviert. Die mitgelieferte Datei zephyr.elf st eine Referenezimplementierung (unter 64 Bit Ubuntu 20.04, zum Beispiel auch unter Windows 10 / WSL lauffähig). Eine korrekte Lösung verhält sich wie in diesem Dokument beschrieben.

1.1 Aufgaben und Eigenschaften des Krypto Prozessors

Der Kyprto Prozessor kann über eine serielle Schnittstelle angesprochen werden und führt für einen Benutzer AES-128 Operationen durch. Es wird das RTOS Zephyr in Version 2.4.0 als Basis verwendet. Diese Code ist damit prinzipiell auf einer Reihe von Microcontroller lauffähig. Wir verwenden als "Microcontroller Boardëin 64bit Linux (board **native_posix_64** in Zephyr Sprech). Da wird für die Linux Entwicklung keine SDKs benötigen muss dieses auch nicht installiert werden. Geben Sie beim Erzeugen der Buildumgebung daher bitte (**CROSS_COMPILE**= und **ZEPHYR_TOOLCHAIN_VARIANT=cross-compile**) an.

Das native_posix_64 Board implementiert eine virtuelle serielle Schnittstelle namens **UART_0**, sowie eine implementierung der crypo API mittels libtinycrypt **CRYPTO_TC**. Diese beiden Treiber sind zu verwenden.