EXAMPLE NAME: CRYPTO_AES_EXAMPLE_XMC45

OVERVIEW: This example uses the CRYPTO_AES APP to perform data encryption for 16 bytes of data using the encryption mode and key set in the APP. At runtime, the encryption mode is reconfigured to decryption mode while maintaining the original key. The data are compared and LED lights up if the data is the same.

DESCRIPTION:

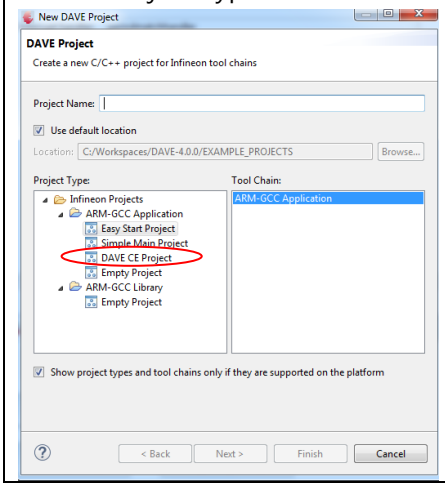
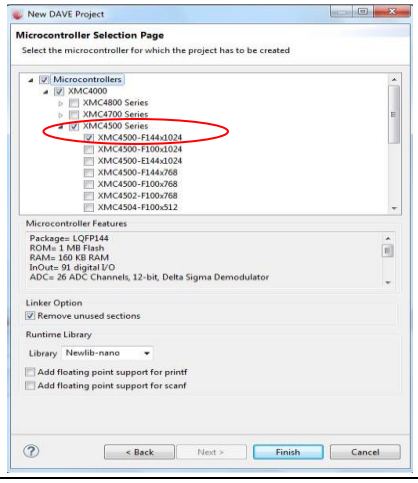
- CRYPTO_AES APP is used to calculate an AES checksum based on a selected AES cipher mode (ECB selected). A 128 bit encryption key (foobarfoobarbaz1) and AES encryption operation is selected.
- DIGITAL_IO APP is used for LED toggling.
- Main program performs data encryption for 16 bytes of data. Using a runtime API, AES operation is changed to decryption mode while maintaining same AES key. The original data is then compared with the decrypted data. LED lights up if the data are the same.

REQUIRMENTS:

Boards Required: XMC4500 CPU Board (Order Nr: KIT_XMC45_EE1_002)

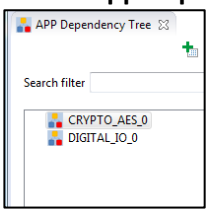
HOW TO CREATE THE PROJECT:

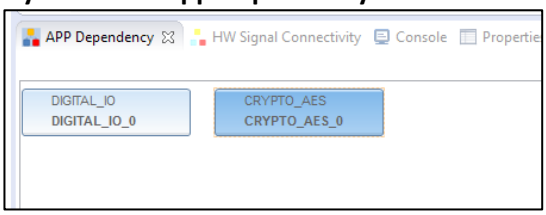
1. Open the DAVE CE and use  "Add IDE New Project Wizard" on the toolbar to add a new DAVE Project.

Enter Project Name Select "Project Type ➔ DAVE CE Project"	Select Microcontroller ➔XMC4500 Series ➔ XMC4500-F144X1024
	

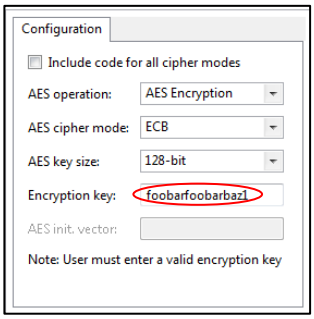
2. Use the  "Add New APP" in the toolbar to add APPs listed. Configure the App instances with the following configurations.

Views: App Dependency Tree and App Dependency

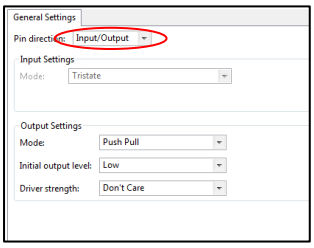




CRYPTO_AES_0:



DIGITAL_IO_0:



3. Use the "Manual Pin Allocator" found in the toolbar, configure the output pin for the LED.

App Instance Name	Resource	Mapped Resource
DIGITAL_IO_0		
	pin	p/3/pad/9

4. Generate the code for configurations made and change main.c accordingly.
5. Build and download to the microcontroller.

HOW TO TEST:

Download and run the demo in the uC.

OBSERVATIONS:

- LED lights up when the result is decrypted correctly.

HINTS WHEN MIGRATING EXAMPLE TO OTHER DEVICES IN THE SAME XMC FAMILY:

No additional information is required.