reverse byte order relative to the payload. For example, using the sample session key from the Bluetooth Core Specification v5.4, Volume 6, Part C, chapter 1.2:

- Session Key (SK): 99AD1B5226A37E3E058E3B8E27C2C666

The KEY.VALUE registers are populated as follows:

- KEY.VALUE[0] = `0x27C2C666`
- KEY.VALUE[1] = `0x058E3B8E`
- KEY.VALUE[2] = `0x26A37E3E`
- KEY.VALUE[3] = `0x99AD1B52`

The same reverse byte order is used for the NONCE.VALUE registers. For the packet example "3. Data packet1" with the following values:

- IV: DEAFBABEBADCAB24
- Direction Bit: 1
- Packet Counter: 1

The NONCE.VALUE registers are populated as follows:

- NONCE.VALUE[0] = `0xBEBAAFDE`
- NONCE.VALUE[1] = `0x24ABDCBA`
- NONCE.VALUE[2] = `0x00000080`
- NONCE.VALUE[3] = `0x00000001`

> **Note:** Although the NONCE in the example above is 13 bytes, it must be written as a 16-byte value with the first 3 bytes zero-padded.

> **Note:** The KEY and NONCE byte order is reversed compared to the NRF52 and NRF53 series devices.

8.4.2.1 Encryption

During packet encryption, CCM will read the unencrypted packet located in memory at the address specified in register IN.PTR, encrypt the packet and append an M byte long message authentication code (MAC) field to the packet.

The message to authenticate and encrypt (m) and additional authenticated data (a) are included in the MAC generation. The first byte in the packet header can be masked by configuring the ADATAMASK register. This is useful for Bluetooth header masking. For protocols other than Bluetooth, the ADATAMASK register must be set to 0xFF for correct CCM operation; the reset value is configured to support Bluetooth.

Encryption is started by triggering the START task with the MODE register set to `Encryption`. The END event will be generated when packet encryption is completed.

The AES CCM will modify the l(c) output field of the packet to adjust for the appended MAC field, that is, add MODE.MACLEN bytes to l(m), and store the resulting packet back into memory at the locations specified in the OUT.PTR list, as illustrated in the following figure. The maximum length of l(m) plus MODE.MACLEN cannot exceed 65535 bytes.