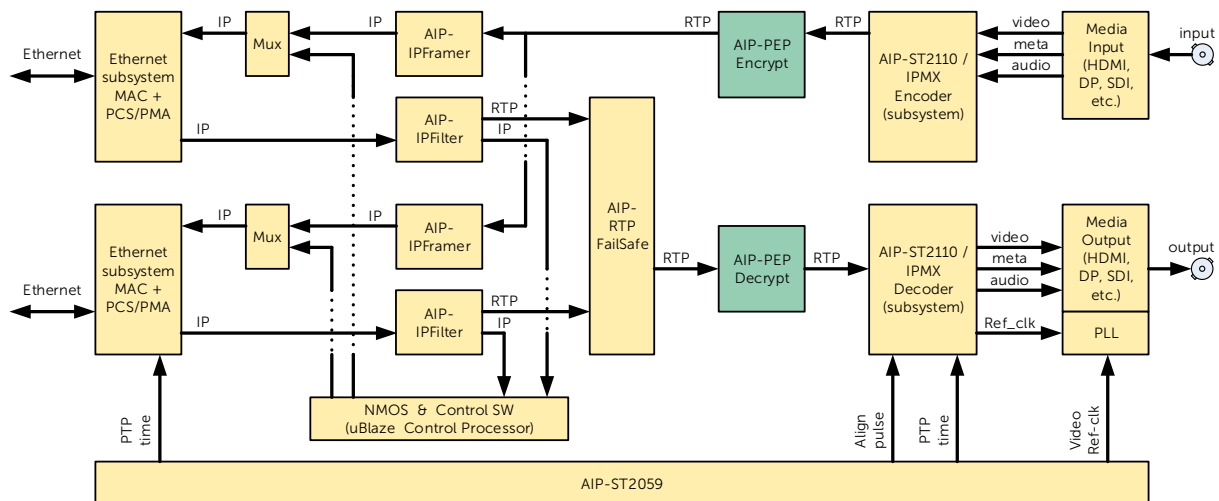


AIP-PEP (Privacy Encryption Protocol)

RTP packet encryption and decryption



The AIP-PEP is an FPGA IP core that enables encryption and decryption of RTP packets. It is typically to be used in, but not limited to, an IPMX media over IP environment.

A single core is able to encrypt or decrypt the RTP payload of multiple streams according to VSF TR-10-13:2024 technical recommendation.

Product Description

The AIP-PEP IP core provides media over IP equipment makers with the ability to securely transport media in order to prevent eavesdropping of the media.

Based on standard AXI4-Stream and AXI4-Lite interfaces, the PEP core can easily be integrated into a media over IP system. The RTL core can be generated using parameter options and is controlled by a software driver and a daemon, which are included.

Key Features & Benefits

- Compliant to VSF TR-10-13
- HDCP Ready* for IPMX HKEP (VSF TR-10-5)
- Supports all RTP streams with fixed payload header size, like ST2110-30,31,40 and JPEG-XS
- Supports ST2110-20 RTP stream with variable payload header size
- Support for AES128 and 256 cipher in CTR mode
- Support for static key version
- Support for up to 64 channels each with unique encryption/decryption parameters
- Support for 128-bit AXI4-Stream bus width
- Configurable RTL implementation to balance resource usage and maximum throughput
- Accumulated bandwidth of > 35Gb/s achievable

Limitations

- Currently, support for ECDH, CMAC, GCM, AAD and dynamic key version is not included

Use cases

- Medical
- Military
- High security Pro-AV
- Broadcast

Available demo design

- The PEP core is integrated in the Adeas IPMX demo design
- Demo design available for AMD ZCU106 development kit

Available documentation

- Product guide

Available licenses

- Site license
- Multi-site license
- Source code license