Conditional Access Secure IP
AS-IP01

Overview

The Abilis Systems CA SecureIP Core is designed for SoC integration on ASICs or FPGAs. It is aimed at processing encrypted MPEG Transport Stream (TS) to deliver corresponding decrypted stream for application devices such as Set Top Boxes (STB).
The CA SecureIP Core integrates hardware advanced security features required to comply with the major digital TV Conditional Access Systems (CAS) providers.
It supports multiple input stream formats as well as multiple stream encryption schemes to comply with stream providers specifications.
A Key Ladder hardware block securely handles secret keys provided by the Smart Card to decrypt the input stream.
The IP has an industry standard AHB bus interface for ease of integration into System-on-Chip (SoC). A DMA interface, master on the AHB bus, allows to transfer streams to/from on-chip host memory with minimal CPU intervention.

Applications

- Set-Top-Box CAS processor ASIC

Benefits

- Shorter **time to market** with a **silicon proven** IP
- Compliant with the latest **Nagravision NOCS1.1** design specifications.
- Compliant with major CAS providers security requirements.

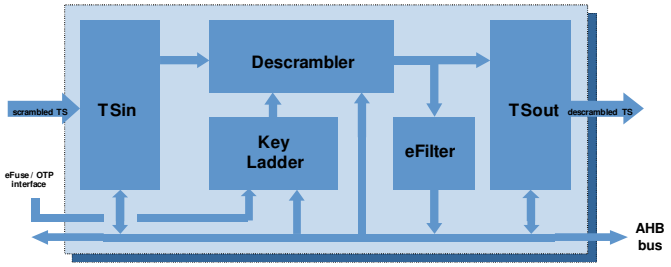

Fig 1 : CA_SecureIP Functional Block Diagram

Features

- **Descrambler Functions**
  - Support DVB-CSA descrambling
  - Support DES ECB/CBC 64 bit key
  - Support TDES ECB/CBC 192 bit key
  - Support TDES ECB-CS for CC2.0
  - Eight Initialization Vector (IV)
  - 8 TDES keys or 32 DES/DVB keys
  - Key Ladder interface
  - Key Ladder Functions
- **"Secret keys" management system**
  - Embedded cipher engine
  - Stream descrambler interface
- **Filter Functions**
  - Support DVB and CC2.0 packets
  - Support 16 simultaneous PID
- **Transport Stream input / output**
  - Support DVB-MPEG TS and CableCard2.0 (CC2.0) packets
  - Support serial and parallel streams
- **AHB interface**
  - Support IPTV stream
  - Support system control

Conditional Access Secure IP
AS-IP01

Functional Description

Stream Input (TSin)
This block supports two data inputs: external TS port and AHB interface.
On TS interface, it receives a data stream through a parallel or serial interface and converts it into a byte wide stream with packet information to be used by the descrambler block. Supported input modes are DVB (188 bytes), and CableCard (200 bytes).
IP variable packet length for IPTV, is possible through AHB interface after software formatting.

Descrambler Engine
Its stream-in interface reads data from the TSin FIFO, analyzes the stream content to extract relevant information, its cipher engine descrambles the incoming stream using DVB-CSA, DES or TDES algorithms. It then forwards the packets to the output stream block.
It receives and securely stores clear control words from the Key Ladder engine. An AHB interface also allows to program control words.

Stream Output (TSout)
This block is located at the end of the stream channel and is aimed at output packets onto external TS port, parallel or serial, in compliance with DVB or Cable Card requirements.
Packets can also be transferred through an AHB slave interface.

AHB Interface
The AHB interface is used to access the various control registers, and to upload or download data stream. The interface is AHB compliant but for the retry and split modes.
This interface can be connected to any AMBA compliant processor interface. A bridge to internal peripheral bus is provided with the IP.

eFilter
This block filters the stream to extract relevant security data, like EMM/ECM, used for stream decryption. The eFilter block is master on the AHB bus

Key Ladder
The purpose of the Key Ladder is to securely handle secret keys. The Key Ladder is built around a cypher engine processing and deriving keys which are securely applied to the descrambling engine to decrypt the input data stream.
The key ladder functionality is controlled from the OTP / eFuse interface to define the allowed CAS provider configurations.

OTP / eFuse Interface
The Key Ladder is connected to an OTP memory. The OTP memory itself, which is technology dependent is not part of the CA Secure IP, only the OTP interface is provided.
The OTP bits are configuring the Key Ladder to meet CAS providers security requirements.

Software Layers
Some software source code to drive the IP is provided in the documentation.

Deliverables

The CA SecureIP Core is an RTL design in Verilog HDL and VHDL that implements digital TV security features on ASIC or FPGA. The core includes RTL code, test scripts and a test environment for full simulation.