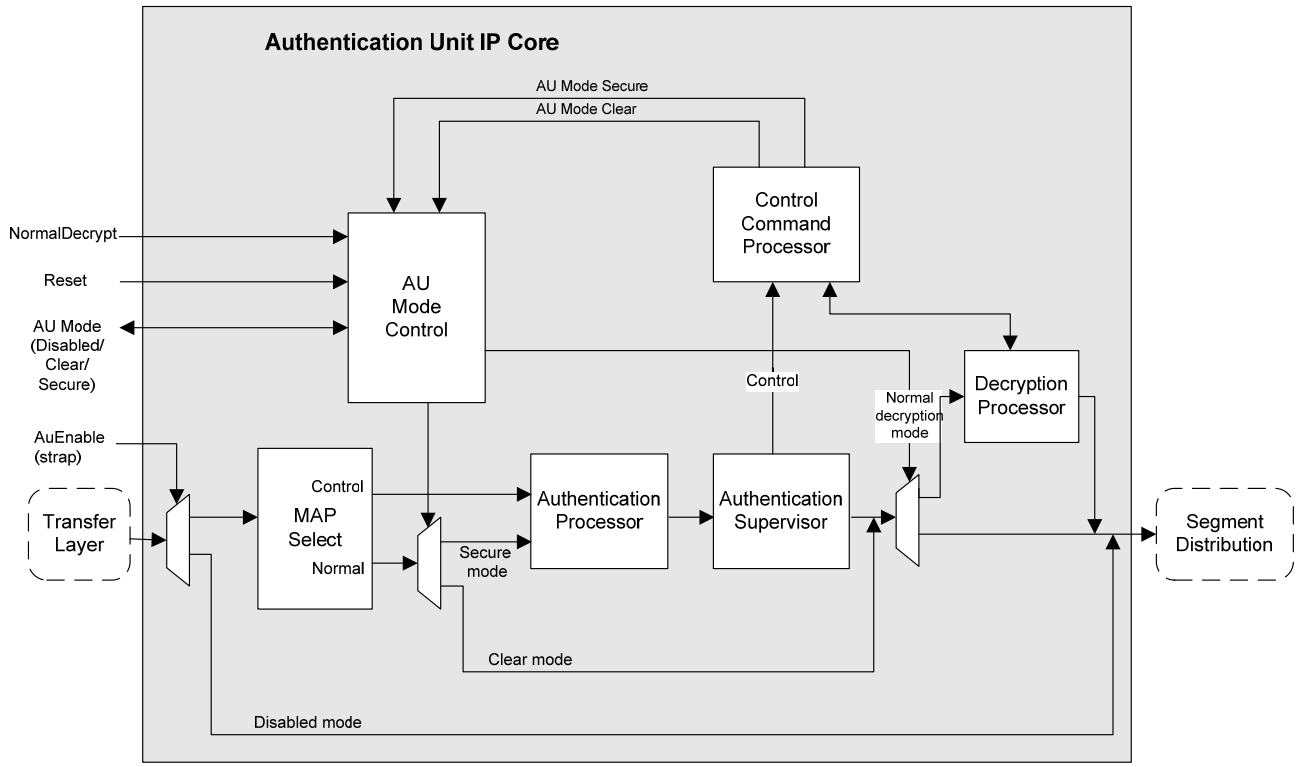
Document Title

Authentication Unit IP Core Product Sheet

The Authentication Unit (AU) Intellectual Property (IP) core is a synthesizable VHDL model that contains functionality for Telecommand (TC) authentication using the Advanced Encryption Standard (AES). The functionality also includes Key management and Logical Authentication Channel) LAC management. The AUIP core is typically located in the TC chain in a Satellite Management Unit (SMU) when authentication of the sender or encryption of TC data is needed.



Features:

- Secure or Clear (transparent) mode
- Mode, Key and Status control via AU TC commands
- Support for 4096 session Keys
- Support for 1024 master Keys

Compatibility:

- Decryption Algorithm, AES (FIPS PUB 197) using 128 bits key length
- Signature validation, AES CMAC
- Decryption of uploaded keys, AES CBC
- Normal decryption commands, AES CBC

RUAG Space AB
Postal address
SE-405 15 Göteborg
Sweden
Telephone
+46 (0)31 735 00 00
Telefax
+46 (0)31 735 40 00
Registered number
556134-2204
VAT number
SE556134220401

1 System Overview

The supported authentication technique is a "plain-text-with-appended-signature" system. It consists of appending a digital signature at the end of the TC Segment, with or without encrypting the data. The signature is a 16-octet value generated from a secret key, the TC Segment and a LAC Counter value. The Authentication Unit regenerates the signature for the received TC Segment, and the command is only accepted if the two signatures match. Three different LAC Counters are provided.

The Authentication Unit IP Core consists of the following logical functions:

- The Authentication Processor, which regenerates a Signature for each authenticated TC Segment and compares it to the Signature provided in the Authentication Tail.
- The Authentication Supervisor, which transfers correctly authenticated TC Segments either to the Segment Distribution after deletion of the Authentication Tail, or to the Control Command Processor.
- Decryption Processor, which decrypts TC segments with encrypted data.
- The Control Command Processor, which executes the AU Control Commands. Encrypted TC segments are decrypted by the Decryption Processor before the commands are executed.

1.1 Main Implementation Blocks of the AUIP

The figure below shows the main implementation blocks of the AUIP.

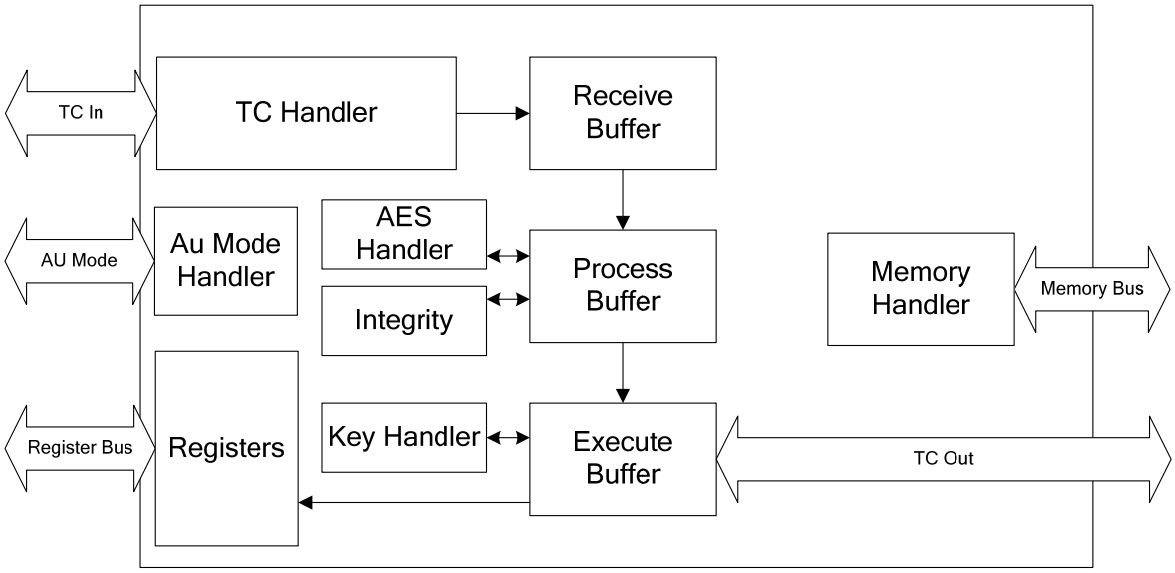


Figure 1-1 Main implementation blocks of the AUIP

The following functionality is included in the AUIP:

- AU Mode interface for changing the AU Mode (Secure (operational) and Clear (transparent))
- Enable input for permanent enabling and disabling of the AUIP
- Enable signal for allowing decryption of normal TC
- TC input for reception of TC segment from the front end user (FEU)
- Abort input for flushing segments blocked by end user
- Memory bus for keys and segment processing
- Segment authentication through AES-CMAC
- Mode, key and status control via AU control TC
- AES-CBC decryption of new keys in AU control TC
- Optional AES-CBC decryption of normal TC
- Provides authenticated and optionally decrypted (normal) TC to the back end user (BEU).
- Allows status register read access via Register bus

1.1.1 TC In

The TC In interface is used for receiving TC segments serially from a front-end-user. The front-end-user can also signal an abort to flush segments blocked by a back-end-user. The abort event is also propagated to the back-end-user

1.1.2 AU Mode

The AU Mode interface is used for switching the operational mode between disabled, clear or secure mode.

1.1.3 Register Bus

The Register Bus interface can be used to monitor the progress of the AUIP, where for example information about accepted and rejected TC segments is found. The interface consists of a select and ready signaling implementation.

1.1.4 Memory Bus

The Memory Bus interface is used for accessing two external memories. One where master keys are located and the other as work area. The interface consists of chip select, request, acknowledge and ready signaling, intended to be connected to a memory controller for the memory selected for the specific implementation.

1.1.5 TC Out

The TC Out interface sends the received TC segments byte streamed and with handshaking to a back-end-user.

1.2 Performance

Performance in terms of frequency and area usage on selected technologies is presented. The figures correspond to pre-layout estimations.

Technology	Frequency	Area
Atmel MH1RT	46.7 MHz	115 kSites
Atmel ATC18	78.8 MHz	1.18 mm^2
Actel RTAX2000	41.8 MHz	11825 Comb, 3592 Seq, 1 RAM
Xilinx Virtex2	99.4 MHz	8225 LUT, 8 RAM

2 AUIP VHDL Source Code

The Authentication Unit IP Core model is written in synthesizable VHDL. The AUIP is an almost fully synchronous design based on a single system clock strategy. The model and testbenches are written according to VHDL'93.

2.1 Packages and libraries, interface port and generic types

The following VHDL packages are used in the AUIP VHDL model:
IEEE.Std_Logic_1164, IEEE.Std_logic_unsigned, IEEE.Numeric_Std. Most AUIP interfaces use the *ulogic* type.
There is one generic used for the top entity in the AUIP model, which decides if synchronous or asynchronous reset is to be used.

2.2 Simulation

A testbench is provided with the AUIP model. The main part of the verification is performed using simulation with systematic test benches, which exercise the tested function with an exhaustive test set where possible. If the test set is too large (e.g. testing all possible blocks of input data) the test set is composed of limiting values (e.g. smallest and largest value), values which provokes a specific behavior and random data sets.

All tests are designed to be Go/NoGo tests i.e. the test bench contain both the input stimuli as well as the expected output result. This allows more exhaustive tests to be performed and also makes regression tests easier to perform.

3 Availability

The AUIP core has been developed by RUAG Space AB. The AUIP core including documentation can be made available by ESA to third party users through a dedicated sublicence agreement, limited to the following purposes:

(a) For activities performed in the frame of an ESA Programme and/or as a Customer Furnished Item attached to an ESA contract
(b) In the frame of GMES Programme/Mission when the recipient is established in an ESA Member or Associated States or EU FP7 Participating States.

The usage of the information by third party may only be granted for dedicated single usage purposes and excluding multiple usage purposes.