ESA Contract 4000109901/13/NL/AK Space Link Security - Cryptographic Processor

The Telemetry and Telecommand Link (TM&TC) is the vital connection between the in-orbit Spacecraft and the Satellite Operator in the Ground Control Centre.

TM&TC link is a critical function providing both visibility of the overall satellite health status and capability to control the spacecraft operations and configuration via proper telecommands. Moreover, it may be used to download payload data as well. Last but not least, TM&TC link is also essential in determining the spacecraft position and velocity.

Therefore it should come as no surprise that, over the years, the Space market witness a growing demand to protect the TM&TC link against threats like eavesdropping, spoofing or even attempts to disrupt or to take control of the Spacecraft asset.

A hard-knapsack based Telecommand authentication function was specified in the old ESA PSS-04-151 Standard, now withdrawn. The PSS authentication algorithm is no longer considered secure today.

The new ECSS Standard System did not pick up and improve the PSS heritage regarding authentication, therefore it left a specification gap that has been filled over the years with project-specific implementations.

Notably Galileo and Copernicus programmes have specified and implemented TM&TC link protection mechanisms to respond to their specific needs and requirements.

In 2015 the gap at Standard Specification level has been filled with the publication of CCSDS 355.0-B-1 Space Data Link Security Protocol.

The aim of this contract is to develop and validate a flexible and configurable CCSDS compliant Cryptographic IP Core implementing authentication and encryption functions based on the state-of-the-art AES Algorithms.

The Cryptographic IP Core will be part of the ESA IP Core Library (https://www.esa.int/Our_Activities/Space_Engineering_Technology/Microelectronics/About_ESA_IP_Cores).

The presentation will describe the Cryptographic IP Core, including the architecture, the interfaces, the functionalities and the configuration capabilities.