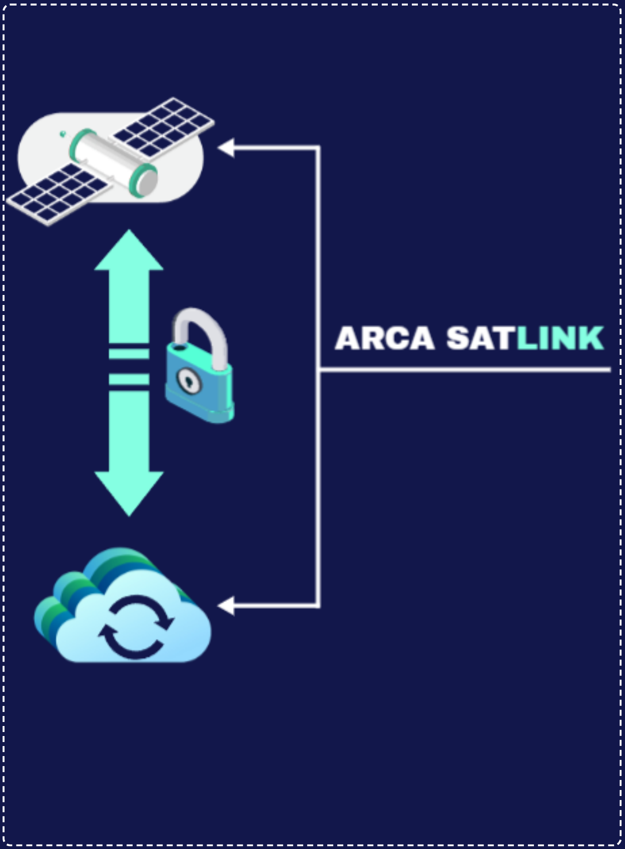
PRODUCT

ARCA SATLINK

End-to-end protection of TMTC and payload data

CYSEC is a European cybersecurity company, headquartered in Switzerland with offices in France, providing innovative software products to protect critical infrastructures on ground and in space.



Today satellite operators of institutional, commercial, and even sometimes governmental missions are still communicating with their spacecraft "in clear", i.e. without implementing any security on the communication links. Unprotected communications for telemetry and telecommand (TMTC) data as well as payload data are making spacecrafts vulnerable to eavesdropping sensitive data all the way to an attacker taking control of the spacecraft.

As a step forward in securing space assets and data, several agencies have added to the CCSDS standards a security extension called the "Space Data Link Security" (SDLS) protocol. SDLS is a protocol to secure communications whose security is applied at the frame level of one or multiple virtual channels, equivalent to a L2 VPN (point-to-point).

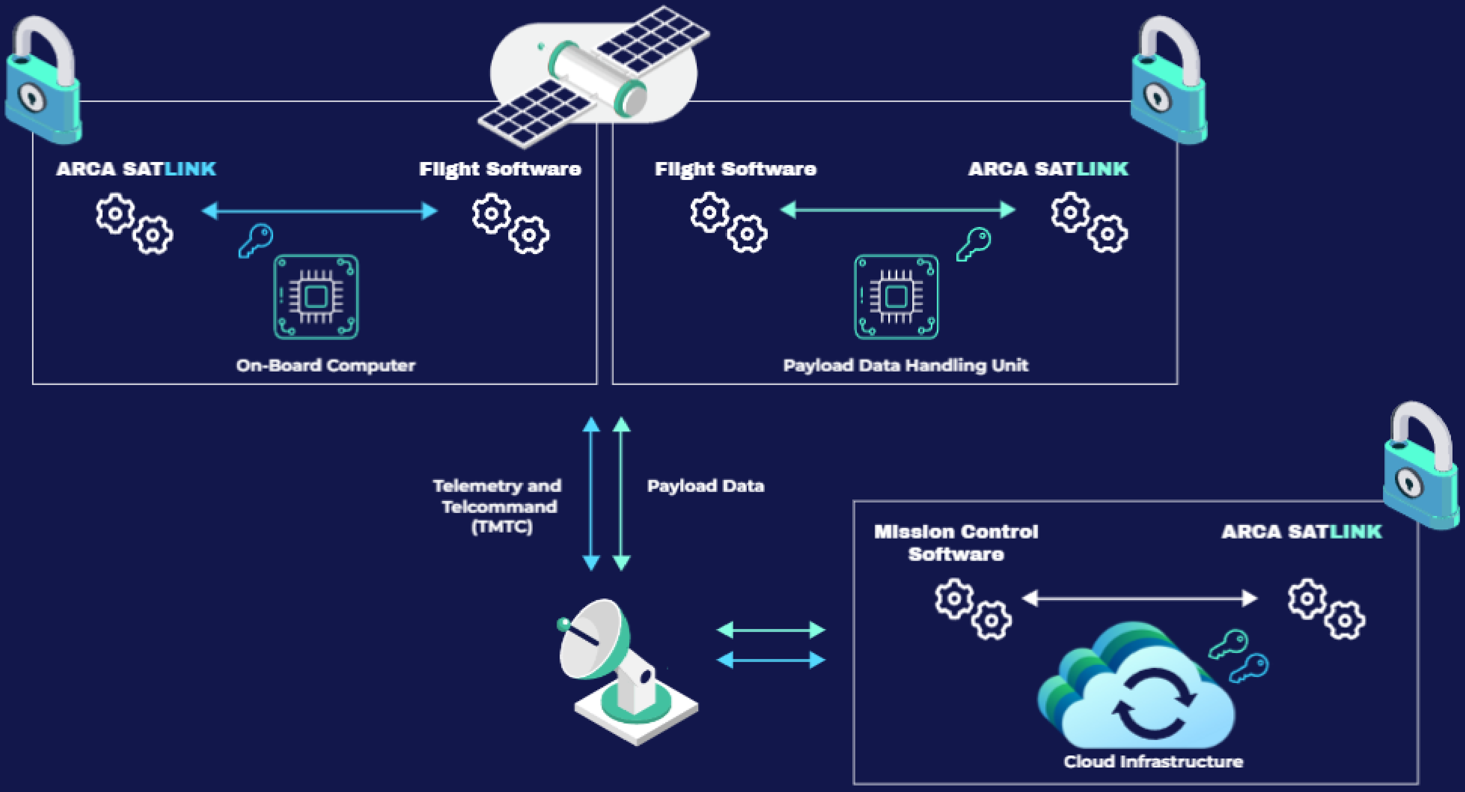
To grow the adoption of SDLS-based security on space comms, CYSEC developed ARCA SATLINK, a software product providing end-to-end protection of TMTC and payload data.

ARCA SATLINK provides all procedures to encrypt, decrypt, authenticate and verify, frames, to manage key lifecycle and virtual channel configuration. It can be applied to satellite communications using CCSDS Space Data Link frames.

CRYPTOGRAPHIC AND KEY MANAGEMENT FUNCTIONS ON GROUND AND ON BOARD

Ground segment and flight software engineers can now integrate ARCA SATLINK cryptographic APIs in their architectures to instantly benefit from SDLS-based security

- End-to-end security with ground and space software components
- Basic cryptographic functions as well as advanced key management functions defined from public SDSL standards
- Independent of communications protocol, CCSDS, CSP or others
- “Dummy-proof” APIs designed for space engineers with no expertise in cryptography
- Include Over-The-Air-Rekeying (OTAR) and key lifecycle management
- Cryptographic and key management functions completed with security associations, anti-reply mitigations, monitoring and control of the datalink



ARCA SATLINK FEATURES

ARCA SATLINK core library contains all 22 functions as described in SDLS standards

ApplySecurity and ProcessSecurity are the two main functions enabling authenticated encryption, e.g. using AES-GCM 256

Designed for minimum footprint on CPU on board

Developed based on ECSS standards

Key generation and key management functions compatible with certified hardware on ground

SDLS FUNCTIONS

Storage

Storage for keys and keys attributes
Storage for virtual channel conf+params (SA)
Storage for SDLS-EP security logs
Storage for ground security logs (generic)

Apply and Process security

Procedures to handle and transform frames
Security reports to logs

Key management service (KMS)

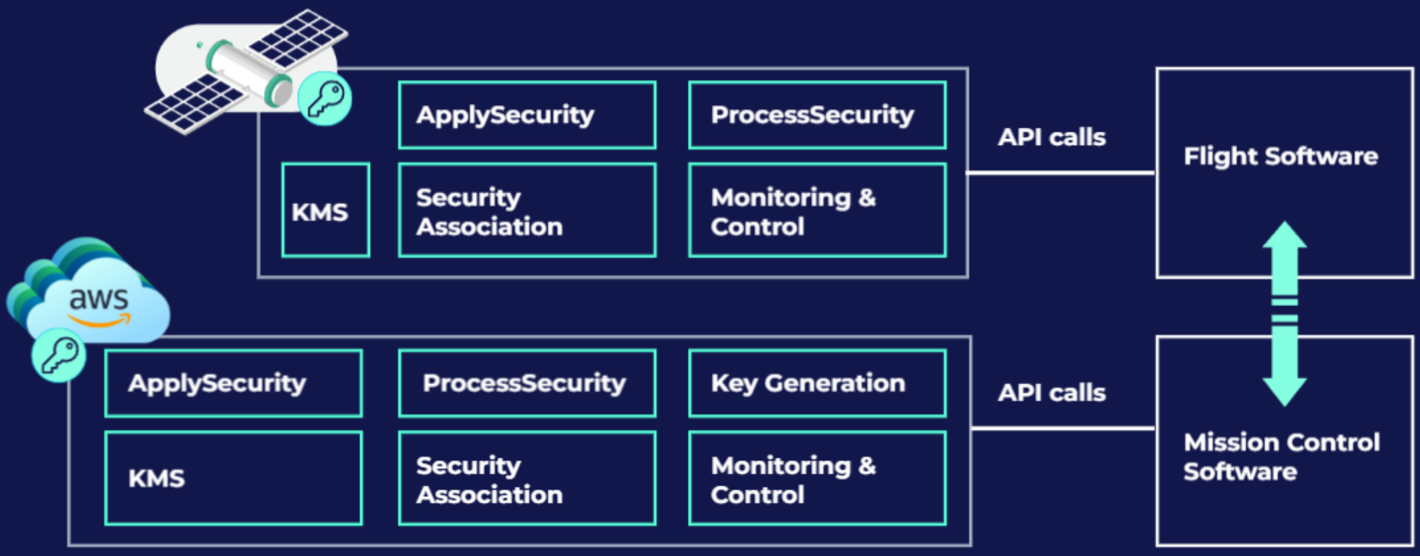
APIs (mission → KMS)
Procedures to generate keys
Procedures manage keys attributes
Procedures to signal key storage changes
Procedures to apply Key storage changes
Procedures to query space key storage
Procedures to answer to key queries
Procedures to return key storage responses

SA management service (SAMS)

APIs (mission → SASM)
Procedures generate / manage SA attributes
Procedures to signal SA changes
Procedures to apply SA changes
Procedures to query space SA
Procedures to answer to SA queries
Procedures to return SA responses

Monitoring and control service (M&C)

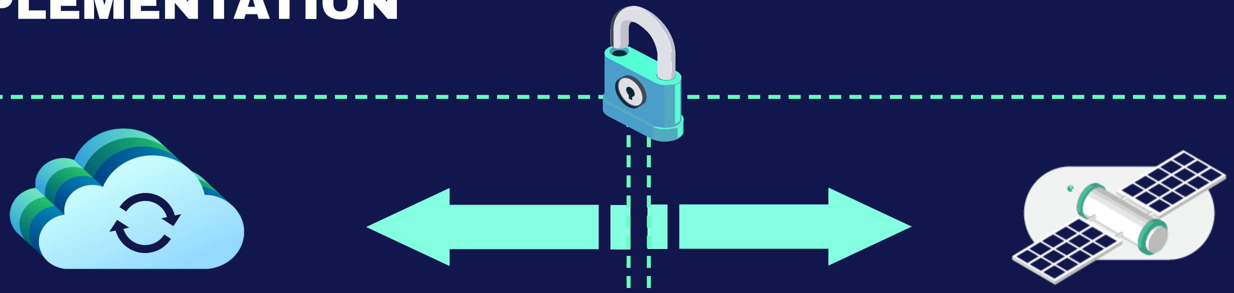
APIs (mission → M&C)
Procedures to query space
Procedures to answer to M&C queries
Procedures to return M&C responses



ApplySecurity
ProcessSecurity
KMS
Security Association
Monitoring & Control
API calls
Flight Software

ApplySecurity
ProcessSecurity
Key Generation
KMS
Security Association
Monitoring & Control
API calls
Mission Control Software

IMPLEMENTATION



GROUND SEGMENT

- ✓ On ground ARCA SATLINK is currently available as a cloud service on AWS or as a library
- ✓ ARCA SATLINK exposes a cryptographic API that can be connected to the mission control software
- ✓ ARCA SATLINK takes advantage of all security features available from cloud providers, e.g. hardware-based key generation and storage, confidential computing Virtual Machines, etc

SPACE SEGMENT

- ✓ On board ARCA SATLINK is currently available as a software library
- ✓ ARCA SATLINK exposes a cryptographic API that can interact with the flight software
- ✓ ARCA SATLINK was developed for Arm-based architectures with Linux or Real-time operating systems

Mathieu BAILLY
VP Sales Space
mathieu.bailly@cysec.com

CYSEC

www.cysec.com/space

EPFL Innovation Park - Building D - CH 1015 Lausanne - Switzerland
257 Boulevard Saint-Germain, 75007 Paris - France