



Secured CCSDS communication with SDLS standard on the
→ new European control centre infrastructure (EGS-CC)

Final Presentation



Benoit Denis
Pierre Denis
Jérémy Gaffarel



Emna Amri
Luca Gambazzi



Ignacio Aguilar Sanchez
Giacomo Da Broi

Table of Contents

- Spacebel
- PROBA
- CCSDS
- SDLS
- Demo
- Conclusion

Spacebel

- IT Systems for the Space sector
- Space and Ground segments
- Mission critical

Space systems and software engineering



Major EU aerospace companies and Space Agencies

- EO monitoring applications
- Geospatial management information
- Environment, resources, and territory management

EO Services



Regional governmental bodies, EC, industry and public users



34 years

> 45 missions

13M€ sales

98% export

Spacebel

SPACEBEL SA



SPACEBEL Vlaanderen NV



SPACEBEL SAS



N7 Space



4 sites

100 staff

500m² clean rooms

ISO9001 2015



PROBA missions



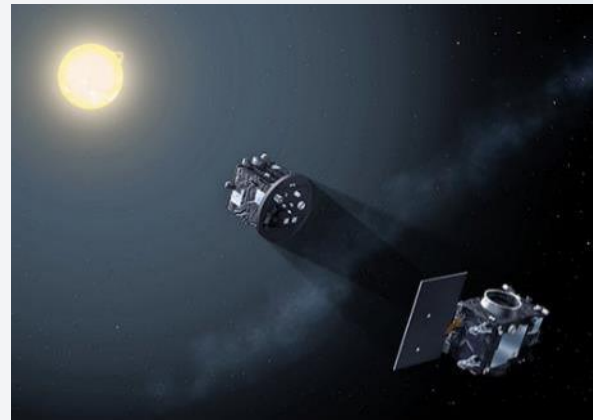
PROBA 1



PROBA 2



PROBA Vegetation



PROBA 3



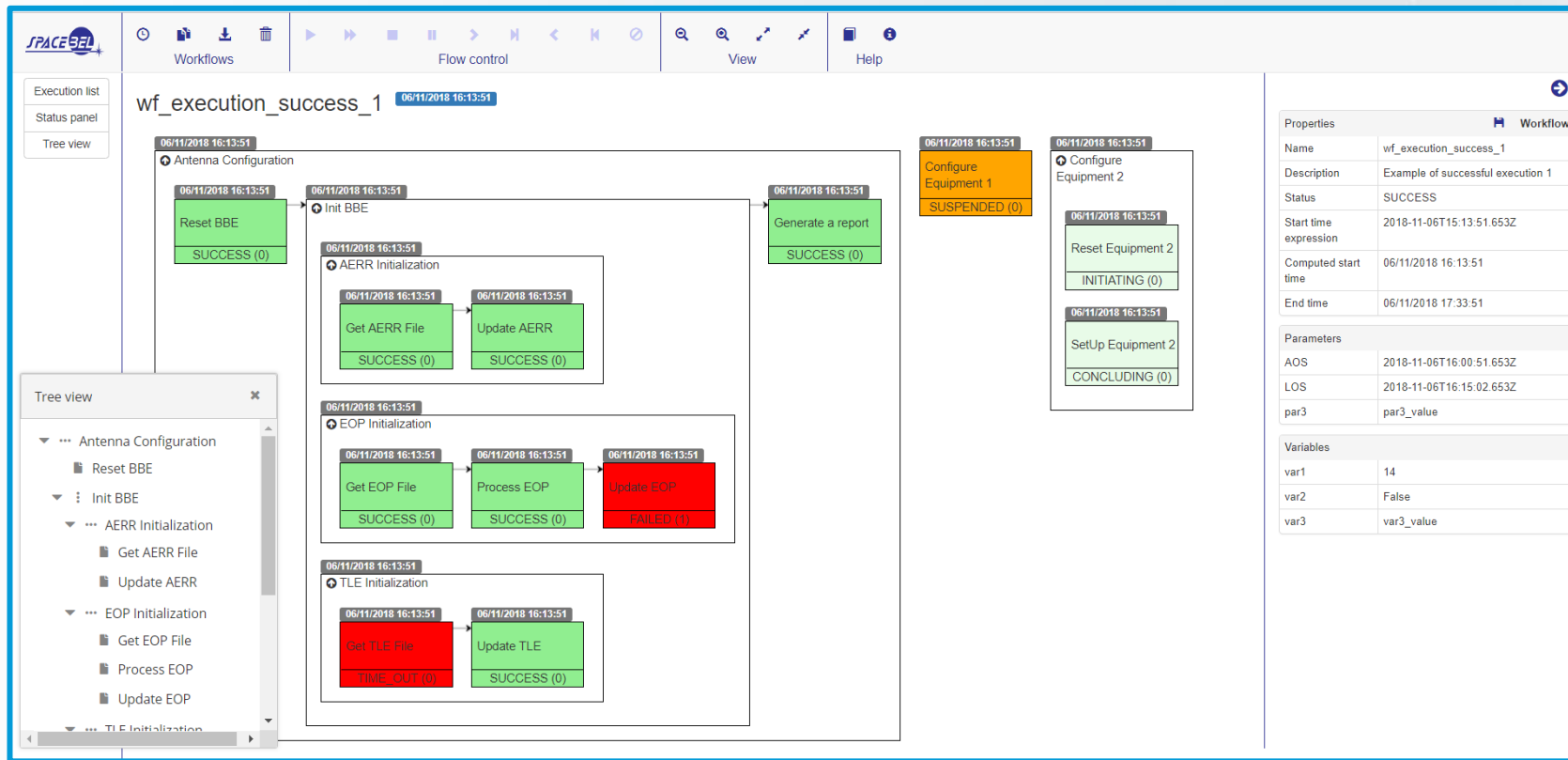
PROBA ALTIUS



PROBA = automation

From planning to pass execution

↪ Workflow Engine



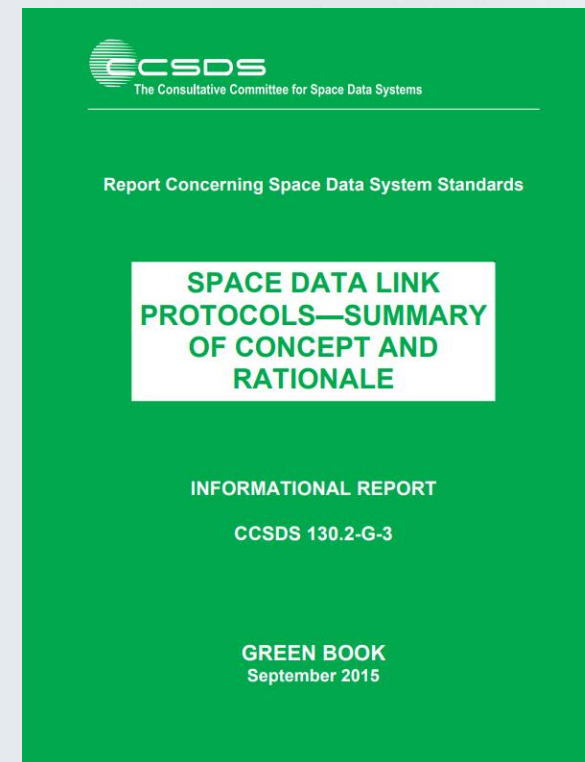
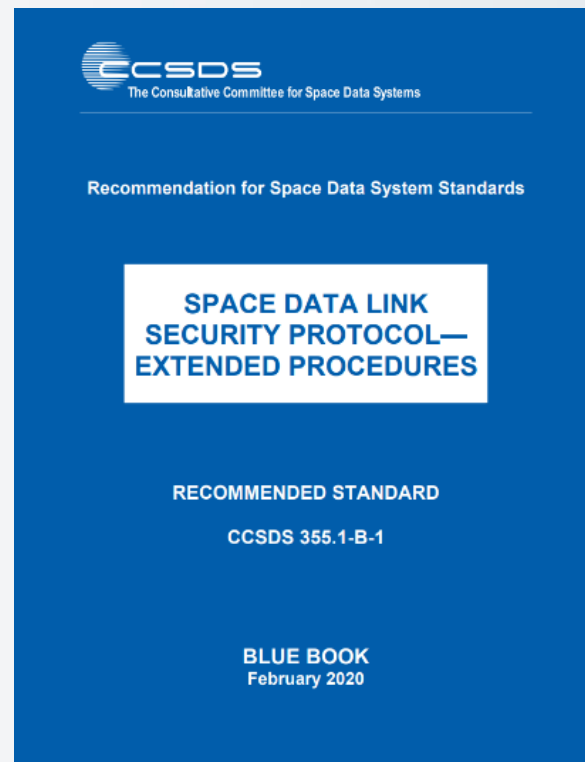
→ Python, Groovy
→ TM/TC link



PROBA = automation

From planning to pass execution

↳ **Workflow Engine**



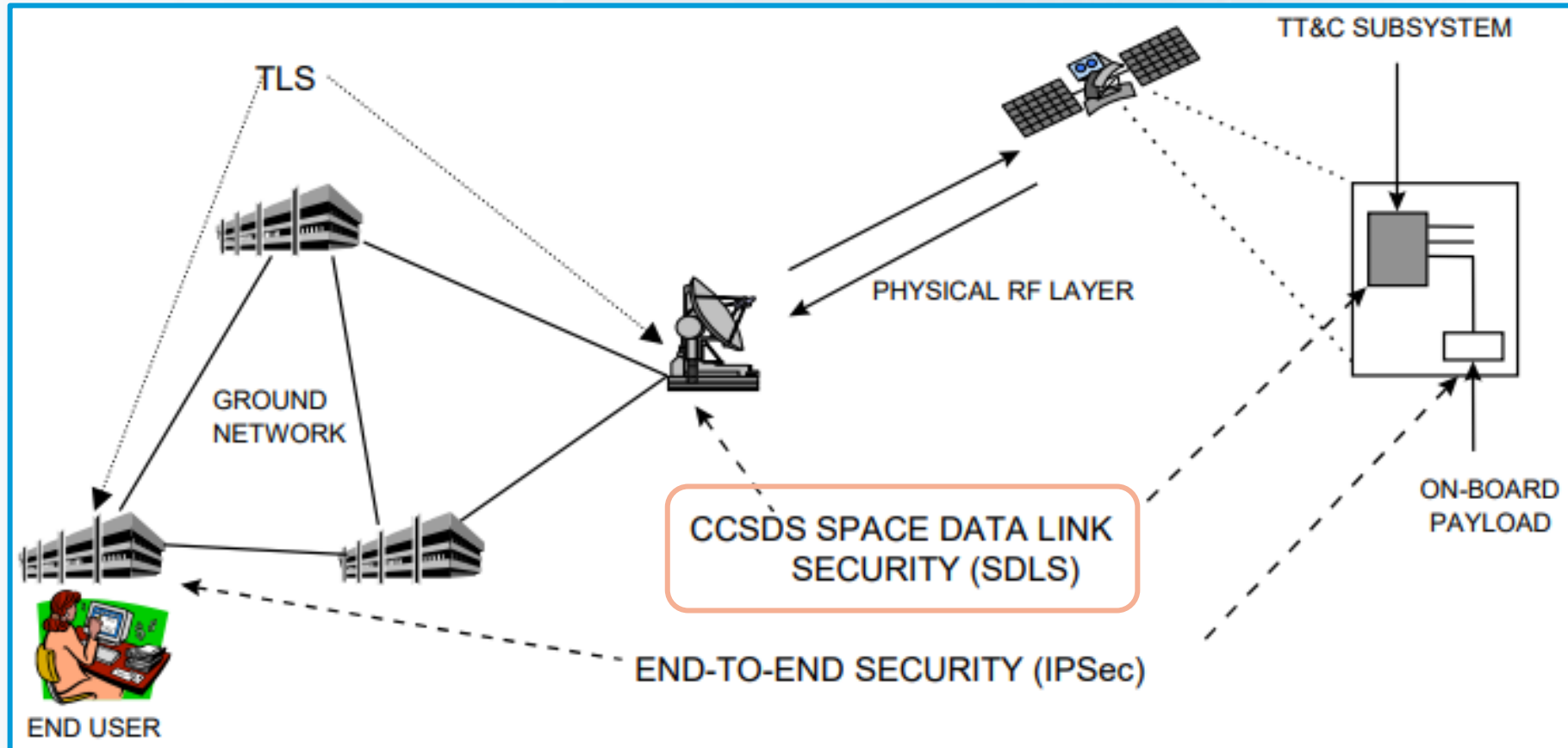
→ Python, Groovy
→ **TM/TC link**

Not encrypted
nor authenticated

**SDLS standard
to the rescue!**



Application to CCSDS protocol

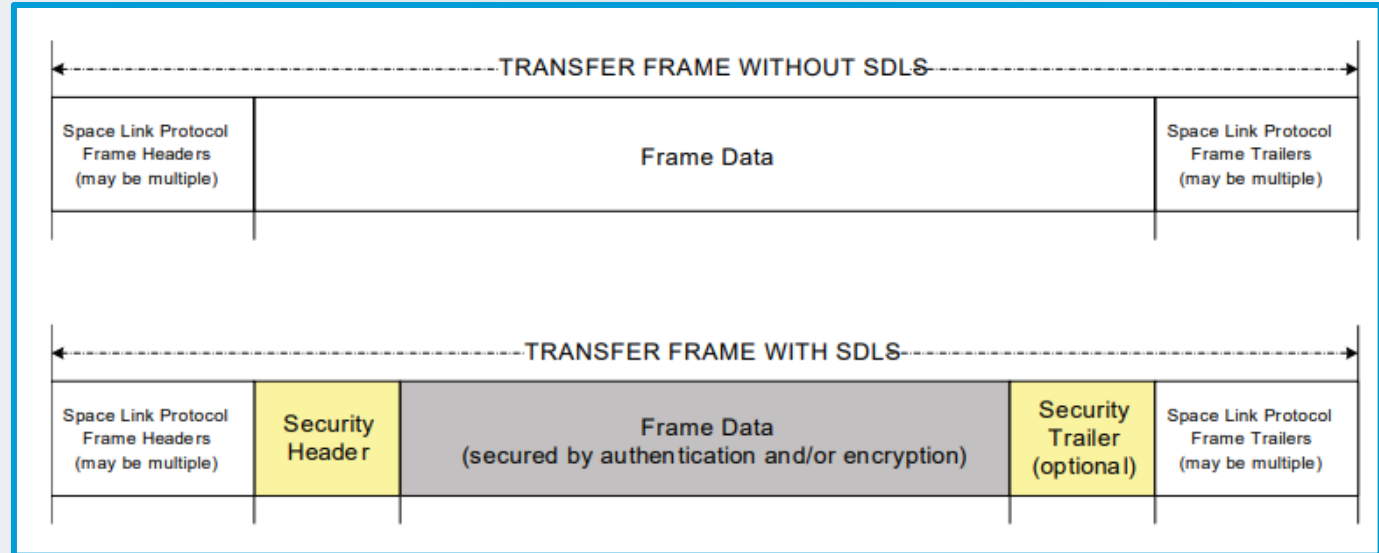


Copyright © 2021 by Spacebel - All rights reserved

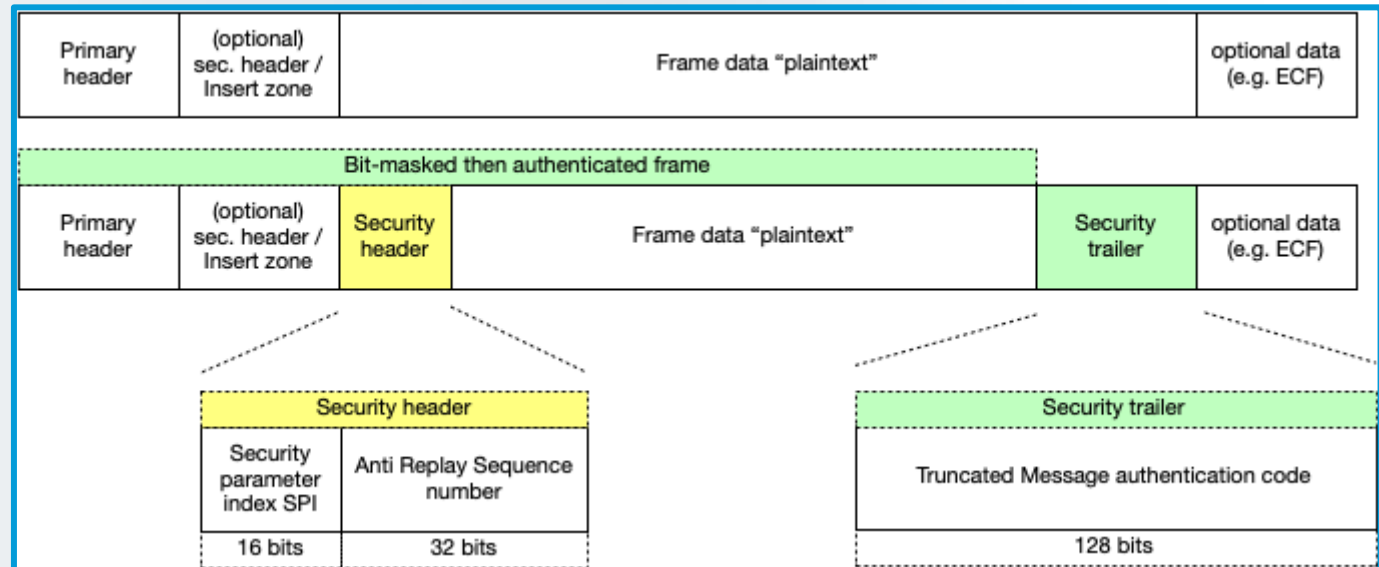


Application to CCSDS protocol

CCSDS frame

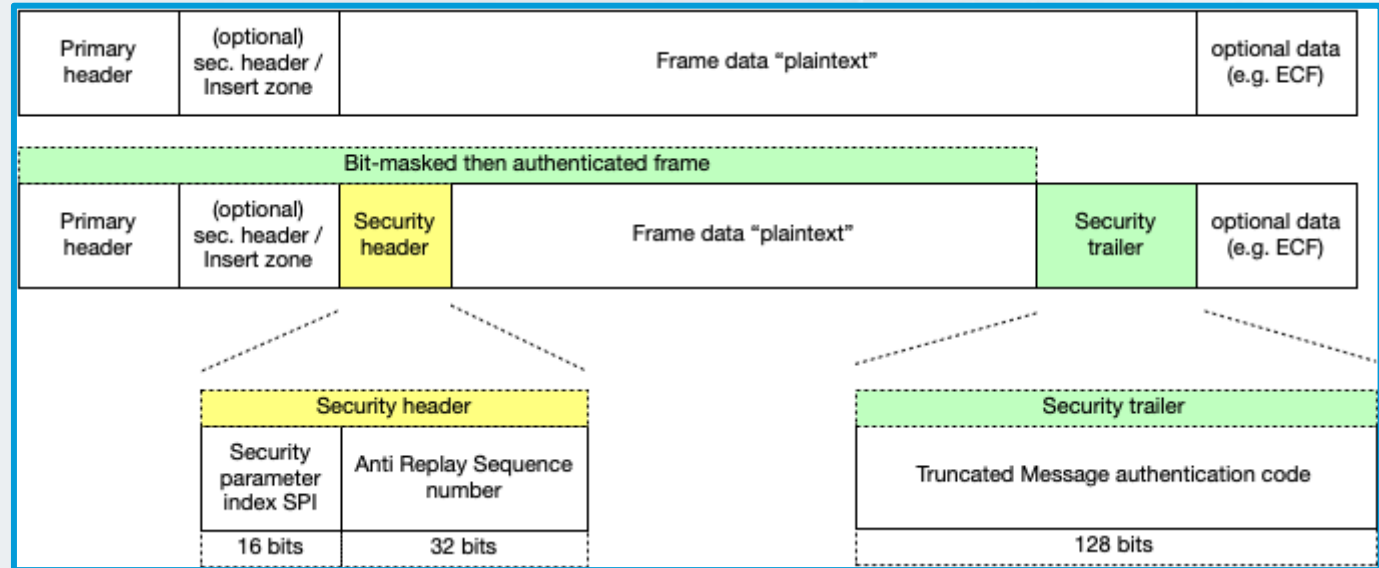


+ authentication

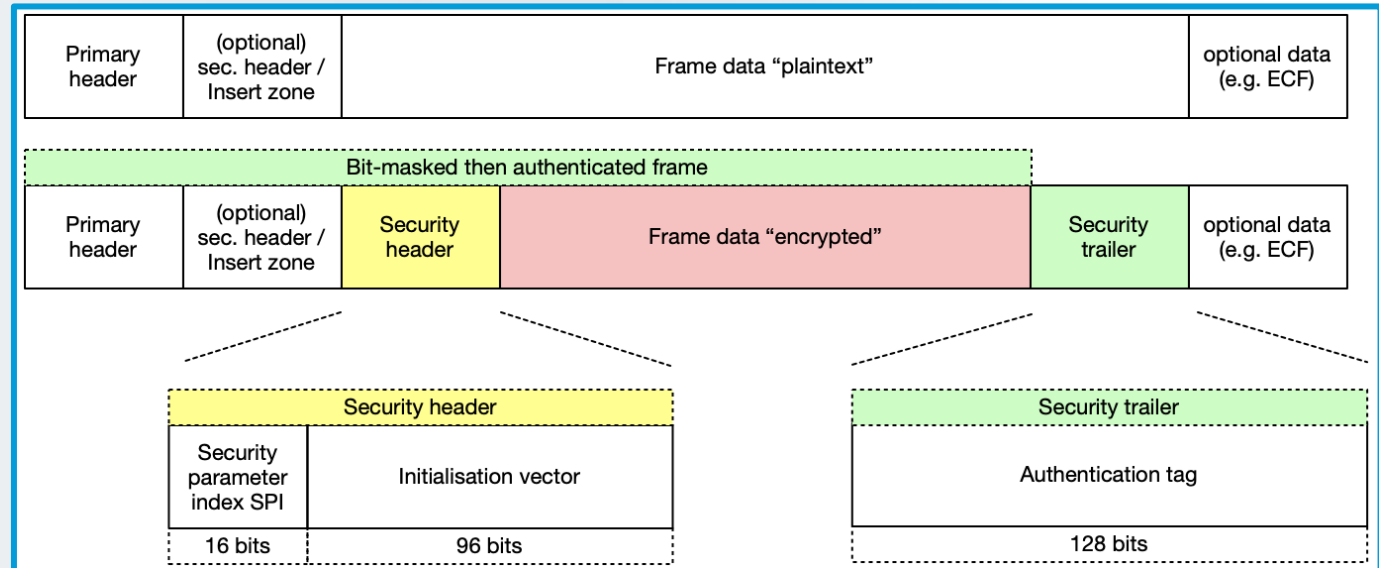


Application to CCSDS protocol

CCSDS frame
+ authentication



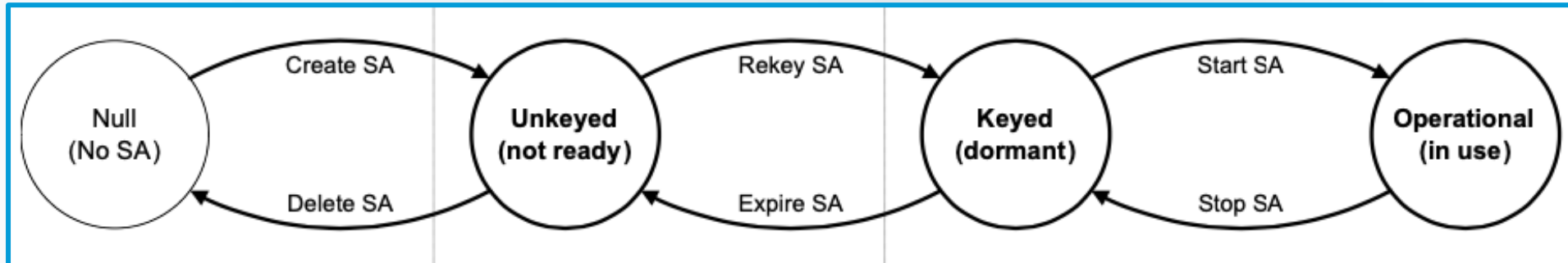
+ encryption



Security Associations

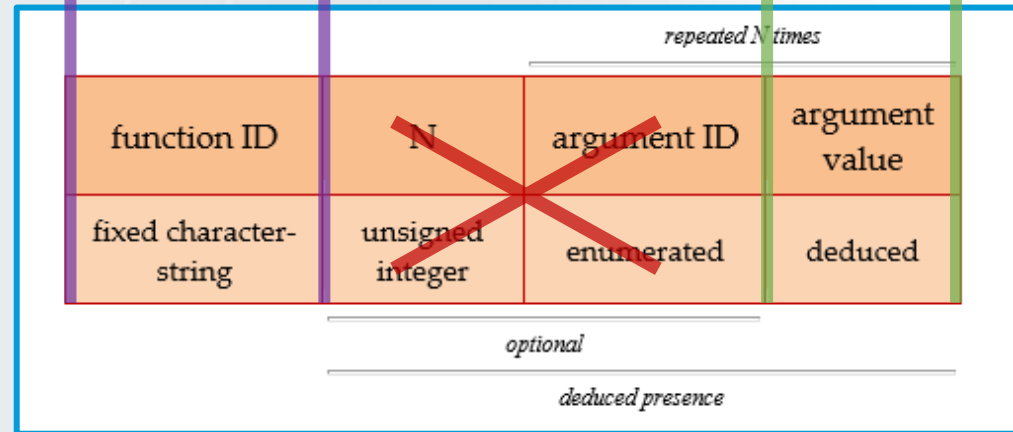
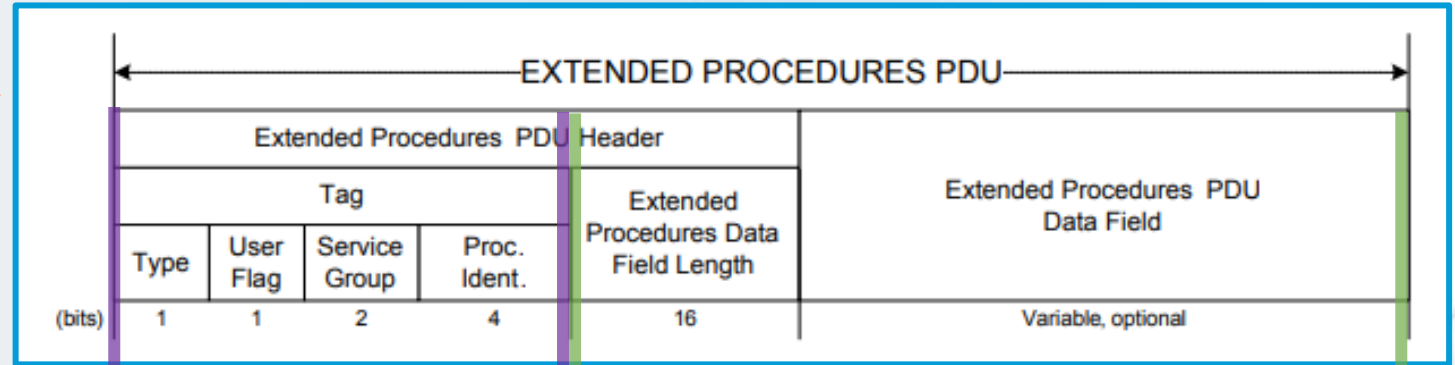
- VC ID
 - MAP ID
- } SA ID

- Encryption key ID
- Authentication key ID
- Initialization Vector
- Sequence Number



Extended Procedures

SDLS EP Service	SDLS EP Procedure
Key Management Service	Key Activation
	Key Deactivation
SA Management Service	Start SA
	Stop SA
	Rekey SA
	Expire SA



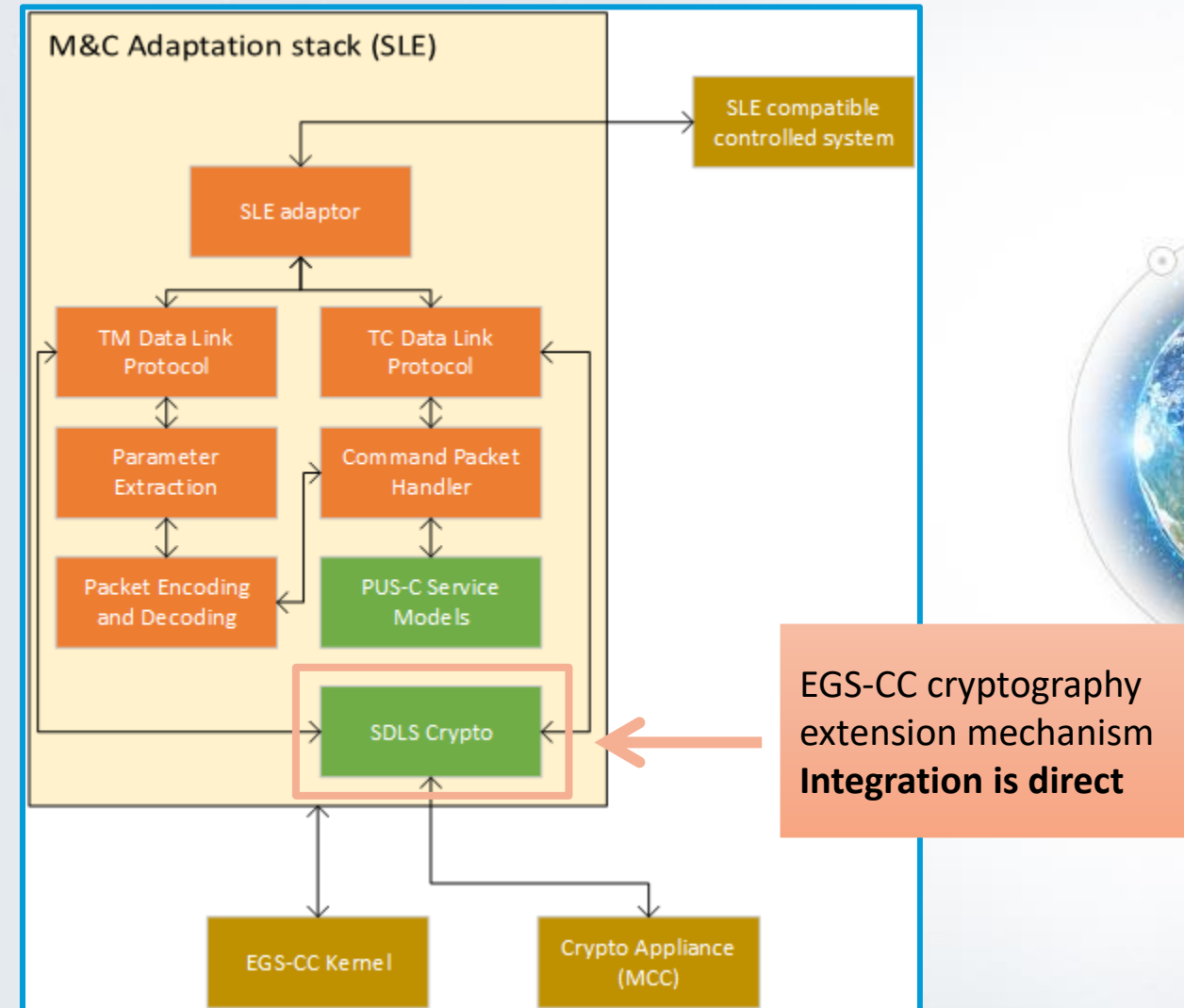
PUS TC[8,1] application data

Prototype

SDLS Crypto architecture in 3 layers:

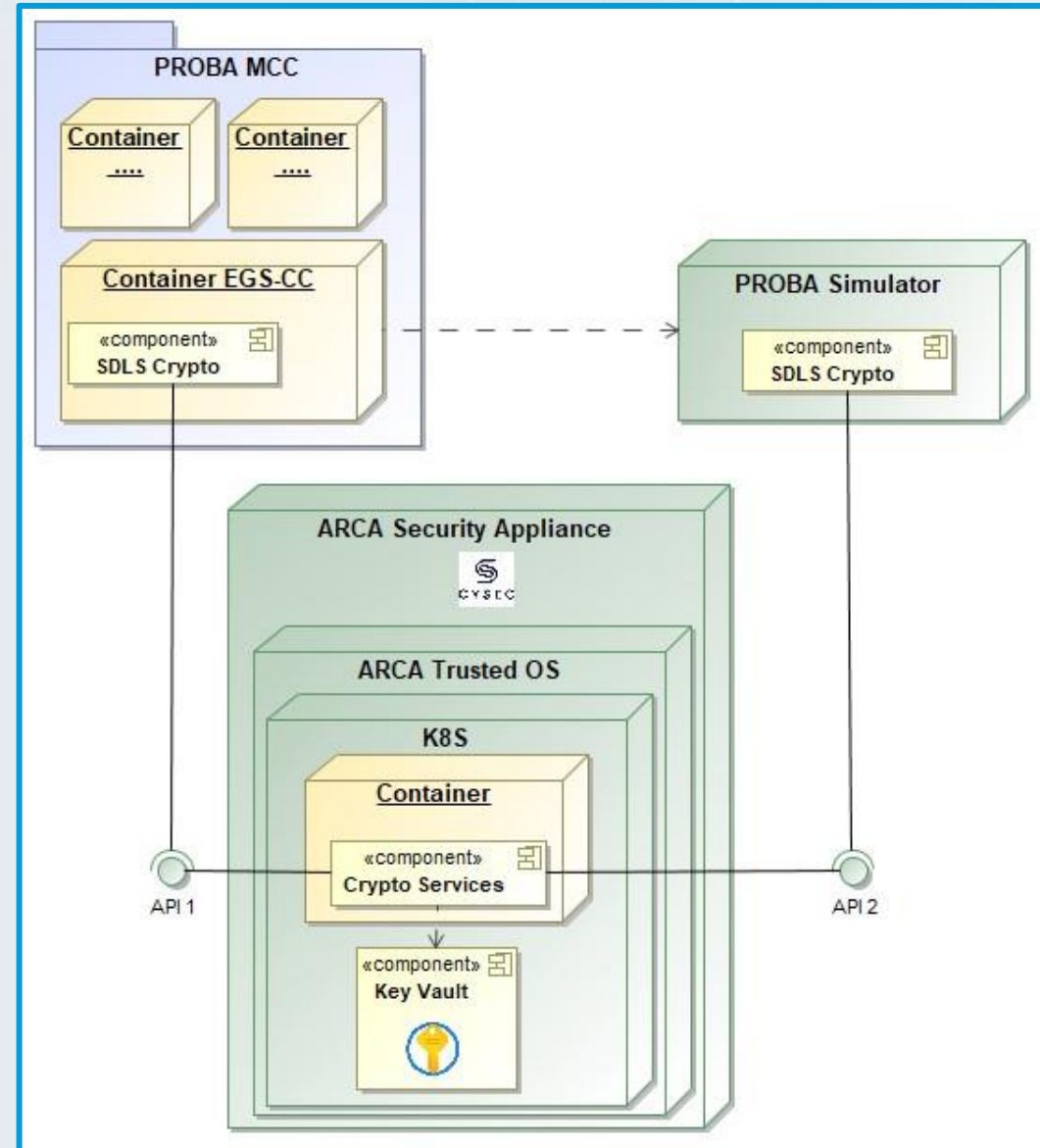
1. Generic logical layer
2. ARCA integration layer
3. EGS-CC integration layer

Reusable with a different crypto appliance and outside of EGS-CC



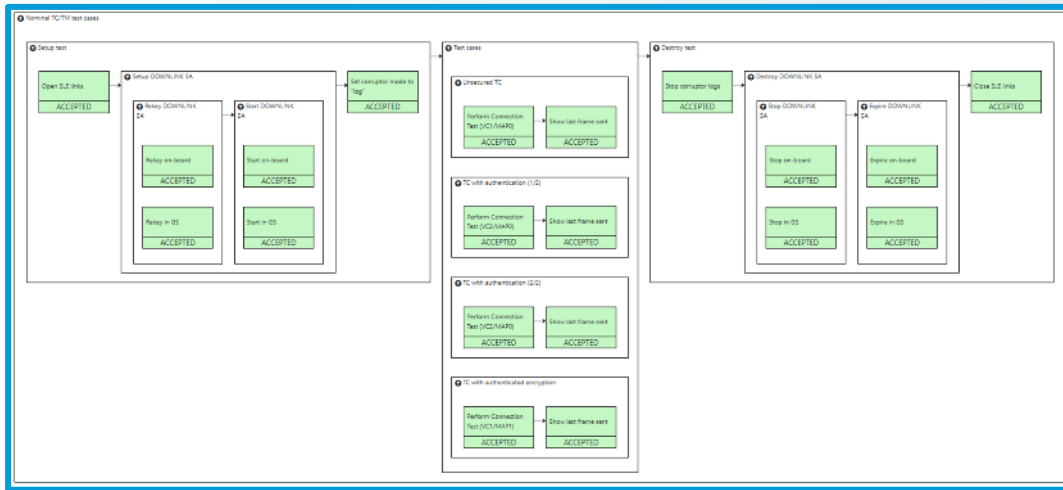
Prototype

- SDLS Crypto component
 - In EGS-CC
 - In PROBA simulator
- 1 ARCA appliance with 2 APIs

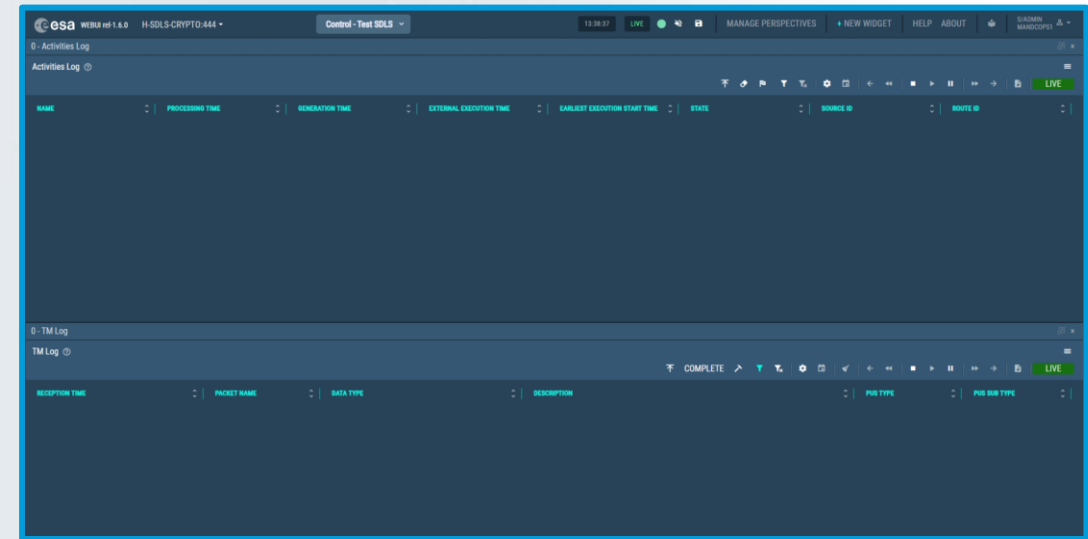


Demonstration

Workflow Engine



EGS-CC Web UI



Conclusions

- Successful exchange of secured TCs and TMs
 - Authenticated
 - Authenticated and encrypted
 - In clear
- Resilient to cyberattacks
 - Repeat attack
 - Incorrect key
 - Clear instead of secured
- Demonstrated Extended Procedures for rekeying
 - Deactivate key
 - Activate key
 - Expire SA
 - Stop SA
 - Start SA
 - Rekey SA
- Successful integration with EGS-CC and ARCA
- Workflow Engine can trigger required EKSE and Python scripts



Recommendations

- Implement all SDLS EP:
 - Keys: OTAR, destruct, verify, inventory
 - SA: create, delete, set ARSN (window)
- Non-fixed ARSN window
- Self-expiring SA
- Hardware-agnostic cryptography
- Integrate with potential KMS
- In-fly demonstration



Questions

Catherine Praile

Business Unit Manager

Mission & Control

catherine.praile@spacebel.be

Jérémie Gaffarel

Space Systems Engineer

Mission & Control

jeremie.gaffarel@spacebel.be