Jet Propulsion Laboratory
California Institute of Technology

Command Encryption with the Advanced Multi-Mission Operations System (AMMOS)

Mike Pajevski
AMMOS Architect
AMMOS Cybersecurity Engineer

March 1, 2023

Jet Propulsion Laboratory
California Institute of Technology

Topics

- Why AMMOS Command Encryption?
- What is AMMOS Command Encryption?
- Concept Diagram
- Internals & Interfaces
- Key Management
- Security Association Management
- Questions & Answers

Jet Propulsion Laboratory
California Institute of Technology

Why AMMOS Command Encryption?

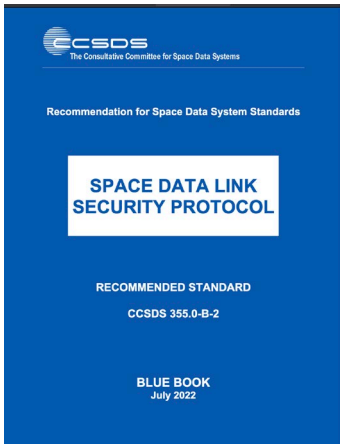
- Unauthorized commanding could jeopardize a mission, and nearby missions
- NASA now requiring command encryption
  - Announcements of Opportunity call out NASA-STD-1006A, Space System Protection Standard
  - Can tailor to accommodate nature of mission
    - *Deep space missions may choose to limit controls applied to the space link if certain controls (e.g., encryption and authentication) pose significant burden to operability or mission success, and if the threat to the space link is low*
- AMMOS Command Encryption provides a <u>multi-mission</u> software solution for NASA robotic missions

Jet Propulsion Laboratory
California Institute of Technology

What is AMMOS Command Encryption?

- Part of the Advanced Multi-Mission Operations System (AMMOS) software
- Multi-mission software solution
  - NASA Class B (unmanned space)
  - Distributed under royalty-free licenses
  - Compiled/tested on RHEL 8
- Applies the CCSDS Blue Book standard Space Data Link Security (SDLS) protocol to Telecommand (TC) transfer frames
  - Frame layer security protocol that leaves headers and error correction field in the clear
  - C, Python, and REST interfaces
- Incorporates the “CryptoLib” SDLS implementation from NASA Independent Verification & Validation (IV&V)

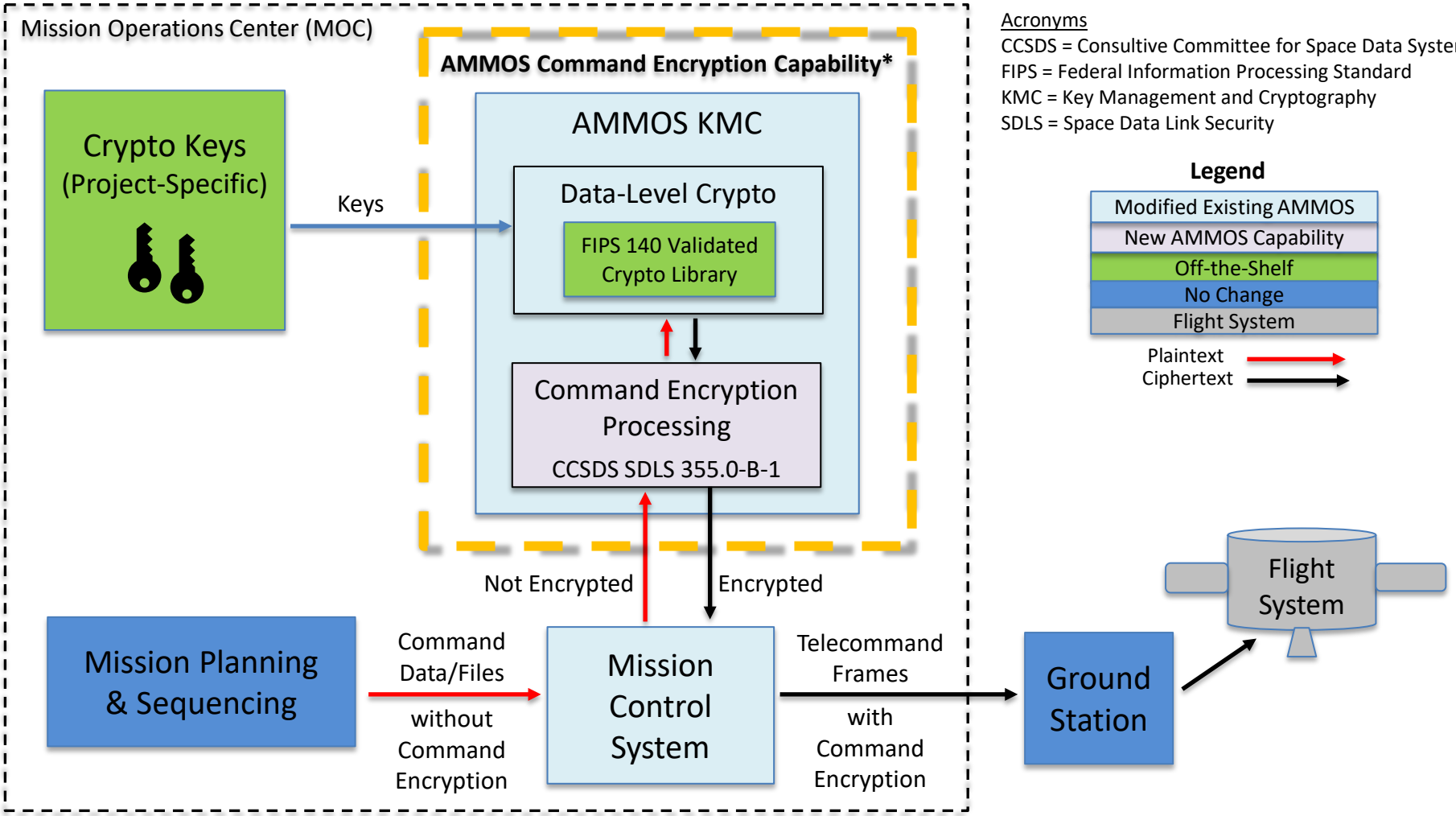
AMMOS
Advanced Multi-Mission Operations System



NASA IV&V’s CryptoLib

Jet Propulsion Laboratory
California Institute of Technology

Conceptual View

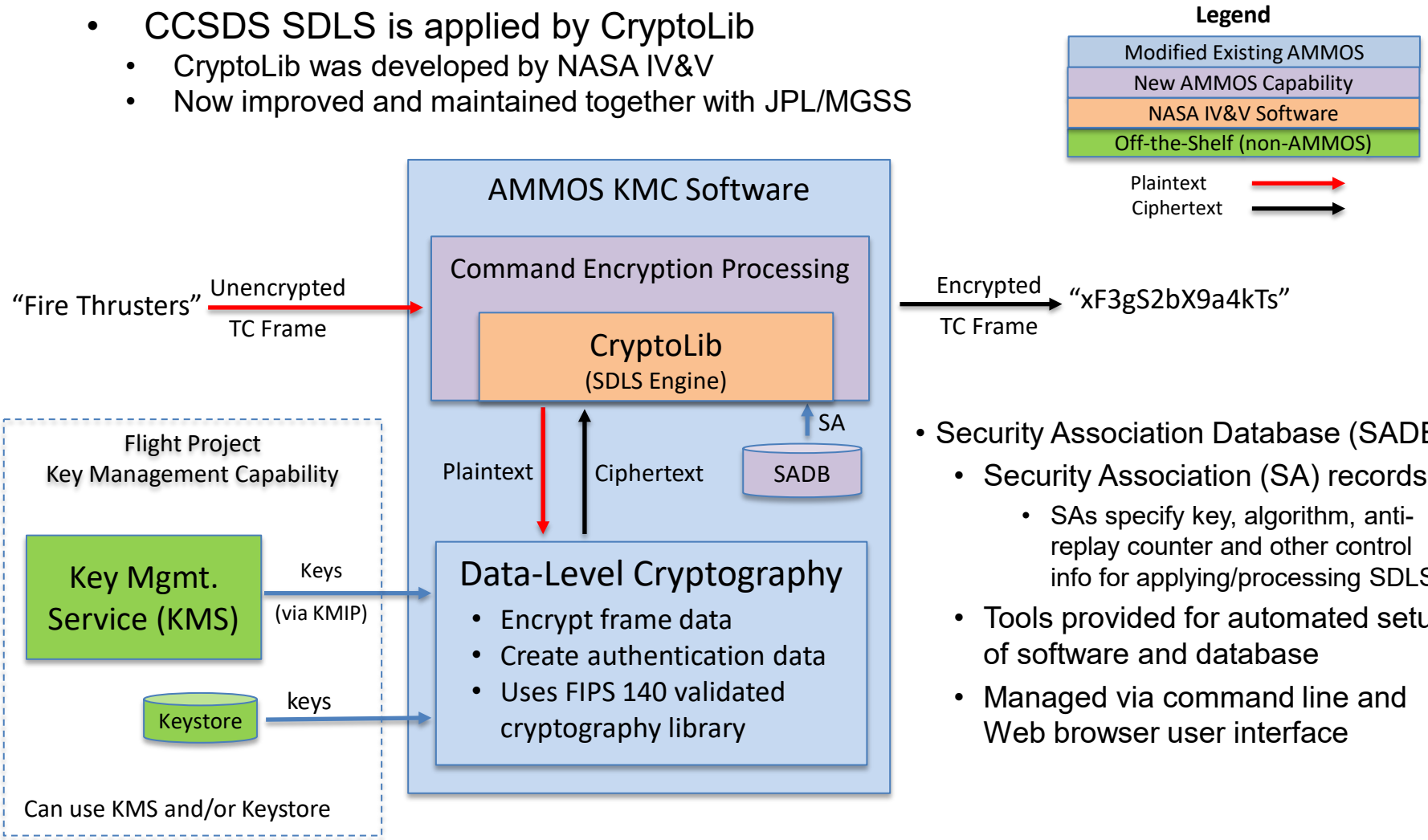


***Multi-mission AMMOS capability that works not only with the AMMOS, but with other mission control systems too.**

Jet Propulsion Laboratory
California Institute of Technology

AMMOS Command Encryption Internals

- CCSDS SDLS is applied by CryptoLib
  - CryptoLib was developed by NASA IV&V
  - Now improved and maintained together with JPL/MGSS



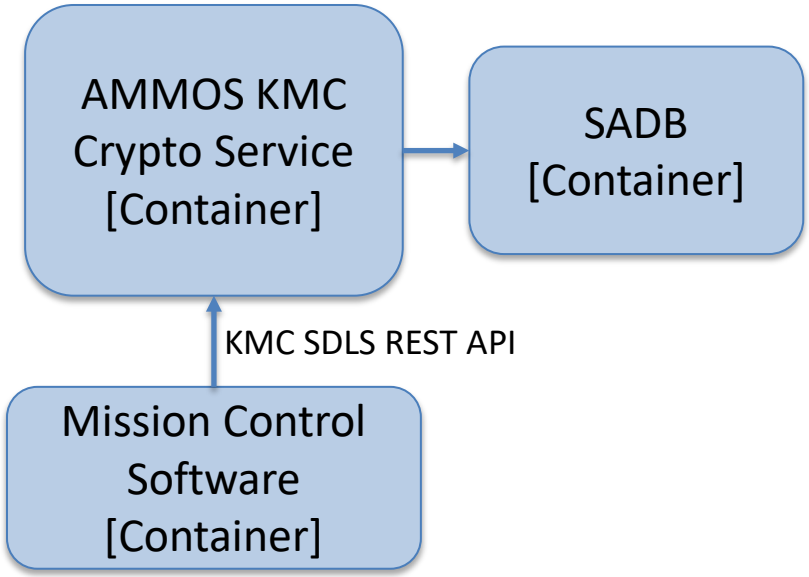
- Security Association Database (SADB)
  - Security Association (SA) records
    - SAs specify key, algorithm, anti-replay counter and other control info for applying/processing SDLS
  - Tools provided for automated setup of software and database
  - Managed via command line and Web browser user interface

Jet Propulsion Laboratory
California Institute of Technology

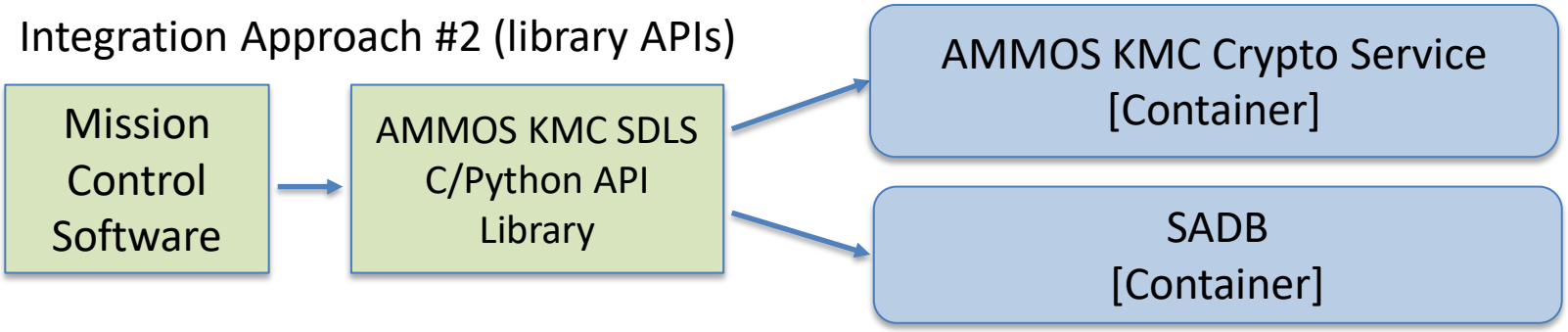
AMMOS Command Encryption Interfaces

- AMMOS KMC provides C, Python and REST APIs for SDLS ApplySecurity and ProcessSecurity
  - SDLS REST API provided by KMC Crypto Service
- SDLS capabilities uses data-level crypto of Crypto Service
- Mariadb is used for SADB

Integration Approach #1 (REST API)



Integration Approach #2 (library APIs)



Jet Propulsion Laboratory
California Institute of Technology

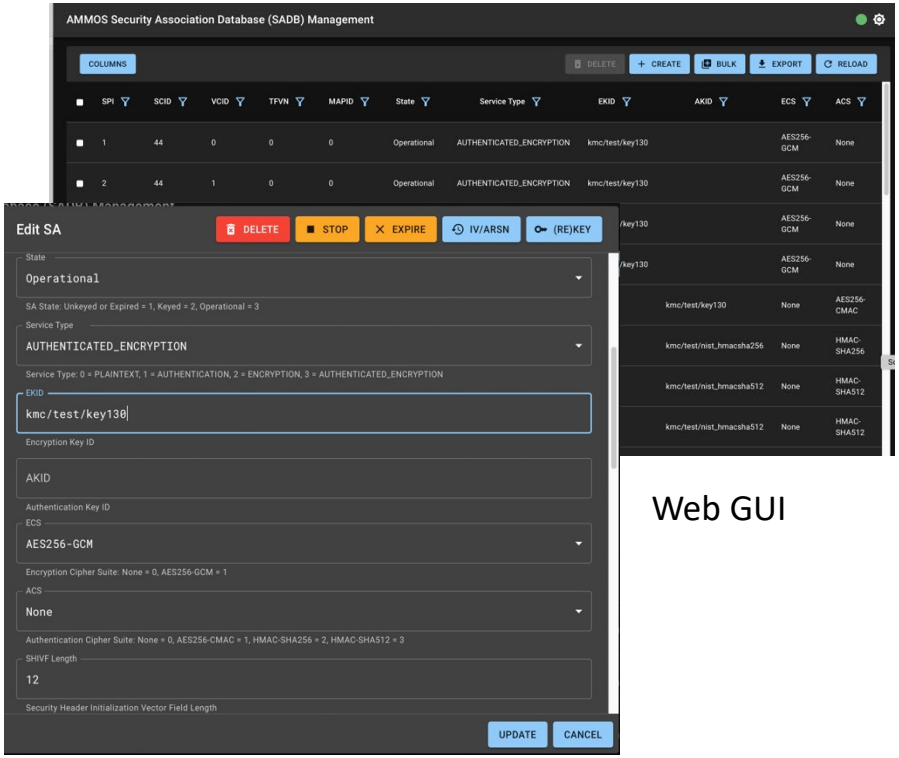
Key Management

- Data-level crypto in KMC can use a Key Management Service (KMS) and/or PKCS-12 keystore
  - Interface to the KMS uses the Key Management Interoperability Protocol (KMIP) standard
  - KMS products can be used, but are not provided, by AMMOS
    - Commercial products are available
  - KMC includes a tool to import hex keys into a PKCS-12 keystore
  - Other tools for creating/updating keystores are available in the operating system and commercially available products
- Crypto keys are project-specific
  - Projects must follow institutional requirements, processes etc.
  - Projects must plan, implement, perform & audit key management
  - Understand available institutional support

Jet Propulsion Laboratory
California Institute of Technology

SA Management

AMMOS includes tools for managing command encryption “Security Associations (SAs)”



Web GUI

```
[pajevski@asec-cmdenc-test-srv1 bin]$ ./kmc-sa-mgmt -h
Usage: kmc-sa-mgmt [-hV] [COMMAND]
KMC Security Association Management CLI
  -h, --help      Show this help message and exit.
  -V, --version   Print version information and exit.
Commands:
  list    List security associations
  create  Create a new Security Association
  update  Update an existing Security Association
  delete  Delete a Security Association
  key     Key or rekey a Security Association
  start   Start a Security Assocation. Only one (1) SA can be active per (SPI,
            GVCID) permutation
  stop    Stop a Security Association
  expire  Expire a Security Assocation
[pajevski@asec-cmdenc-test-srv1 bin]$
```

Command Line Interface (CLI)

Security Association (SA) specifies the crypto algorithm, crypto key, and SDLS options to use

Jet Propulsion Laboratory
California Institute of Technology

Questions?

Jet Propulsion Laboratory
California Institute of Technology

Backup

- Acronyms
- TC Transfer Frame with SDLS
- Relevant Resources
- Acknowledgements
- Additional Authors

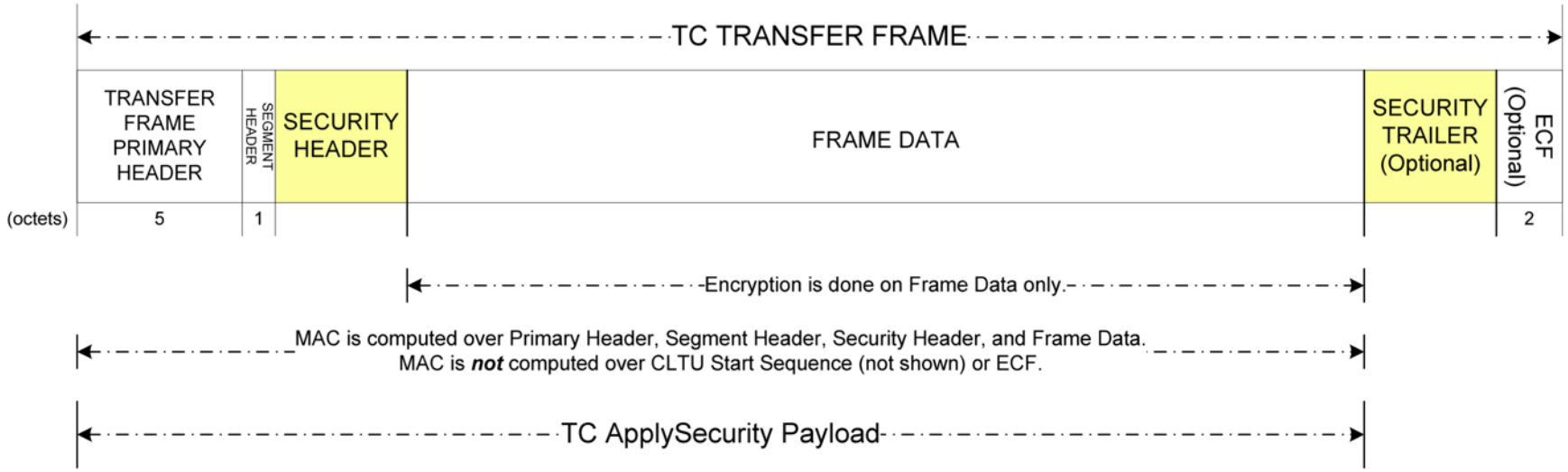
Jet Propulsion Laboratory
California Institute of Technology

Acronyms

Acronym	Definition
AMMOS	Advanced Multi-Mission Operations System
ARC	Ames Research Center
CCSDS	Consultive Committee for Space Data Systems
CLI	Command Line Interface
DTN	Delay (or Disruption) Tolerant Networking
GSFC	Goddard Space Flight Center
GUI	Graphical User Interface
ITOS	Integrated Test and Operations System
IV&V	Independent Verification & Validation
LTB	Lunar Trailblazer
MGSS	Multi-mission Ground Systems & Services
NASA	National Aeronautics and Space Administration
RHEL	Red Hat Enterprise Linux
SA	Security Association
SADB	Security Association Database
SDLS	Space Data Link Security
SMD	Science Mission Directorate
TC	TeleCommand
vMMOC	Virtual Multi-Mission Operations Center

Jet Propulsion Laboratory
California Institute of Technology

TC Transfer Frame With SDLS



- SDLS adds a Security Header and (if authentication is used) a Security Trailer.
  - Lengths are set by each project, and remain constant for a virtual channel
- SDLS (if encryption is used) encrypts the frame data (i.e., payload)
  - Error Correction Field (ECF) left in the clear
- Authentication (if used) is done for headers and (encrypted) payload
- SDLS has the following Security Types (i.e., crypto to perform):
  - Authentication, Encryption, and Authenticated Encryption (i.e., both)
  - Also a Plaintext type, with Security Header but no encryption/authentication

Jet Propulsion Laboratory
California Institute of Technology

Relevant Resources

- Some relevant CCSDS documents are:

Title and URL	Document Number
Space Data Link Security Protocol (https://public.ccsds.org/Pubs/355x0b1.pdf)	*Blue Book 355.0-B-1*
Space Data Link Security Protocol - Extended Procedures (https://public.ccsds.org/Pubs/355x1b1.pdf)	*Blue Book 355.1-B-1*
CCSDS Cryptographic Algorithms (https://public.ccsds.org/Pubs/352x0b2.pdf)	*Blue Book 352.0-B-2*
The Application of Security to CCSDS Protocols (https://public.ccsds.org/Pubs/350x0g3.pdf)	*Green Book 350.0-G-3*
CCSDS Space Data Link Security Protocol--Summary of Concept and Rationale (https://public.ccsds.org/Pubs/350x5g1.pdf)	*Green Book 350.5-G-1*

- Also see the following relevant websites:
  - NASA AMMOS Website
    - https://ammos.nasa.gov
  - CCSDS Systems Engineering Area - Security Working Group (SEA-SEC) Home
    - https://cwe.ccsds.org/sea/default.aspx#_SEA-SEC
  - NASA IV&V CryptoLib GitHub Wiki
    - https://github.com/nasa/CryptoLib/wiki

Jet Propulsion Laboratory
California Institute of Technology

Acknowledgements

- NASA Independent Verification & Validation (IV&V)
  - Developed CryptoLib and now jointly improves with JPL/MGSS
- Goddard Space Flight Center (GSFC)
  - Participated in design review, and continue to collaborate
  - virtual Multi-Mission Operations Center (vMMOC) integrated AMMOS Command Encryption with their Integrated Test and Operations System (ITOS)
- SunRISE and Lunar Trailblazer projects at JPL
  - First adopters of AMMOS Command Encryption
  - Demonstrated capability/interoperability in end-to-end testing
- VIPER project at NASA Ames Research Center (ARC)
  - Evaluating AMMOS Command Encryption for likely usage, and collaborating on necessary capabilities, interfaces, etc.

Jet Propulsion Laboratory
California Institute of Technology

Additional Authors

- The following people are major contributors:
  - *Ken Gieselman; AMMOS Application Security (ASEC) Task Manager and Systems Engineer, Jet Propulsion Laboratory, California Institute of Technology; kenneth.g.gieselman@jpl.nasa.gov; (818)354-1251*
  - *Kam Tso; CAM/KMC/SSM Software Developer, Jet Propulsion Laboratory, California Institute of Technology; kam.s.tso@jpl.nasa.gov; (626)390-9838*
  - *Ibraheem Saleh; KMC Software Developer; Jet Propulsion Laboratory, California Institute of Technology; ibraheem.y.saleh@jpl.nasa.gov; (626)517-3943*
  - *JP Pan; KMC Software Developer; Jet Propulsion Laboratory, California Institute of Technology; james.paul.j.pan@jpl.nasa.gov; (818)354-8739*
  - *Robert J. Brown; Software Developer; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; robert.j.brown@nasa.gov*
  - *David C. Cutright; Software Developer; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; david.c.cutright@nasa.gov*
  - *John P. Lucas; Computer Engineer; Deputy ITC Lead; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; john.p.lucas@nasa.gov*
  - *Justin R. Morris; Computer Engineer, ITC Lead, NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; justin.r.morris@nasa.gov*
  - *Scott A. Zemerick, PhD; Systems Engineer, ITC Lead; NASA Independent Verification and Validation (IV&V), Independent Test Capability (ITC) Team; scott.a.zemerick@nasa.gov*