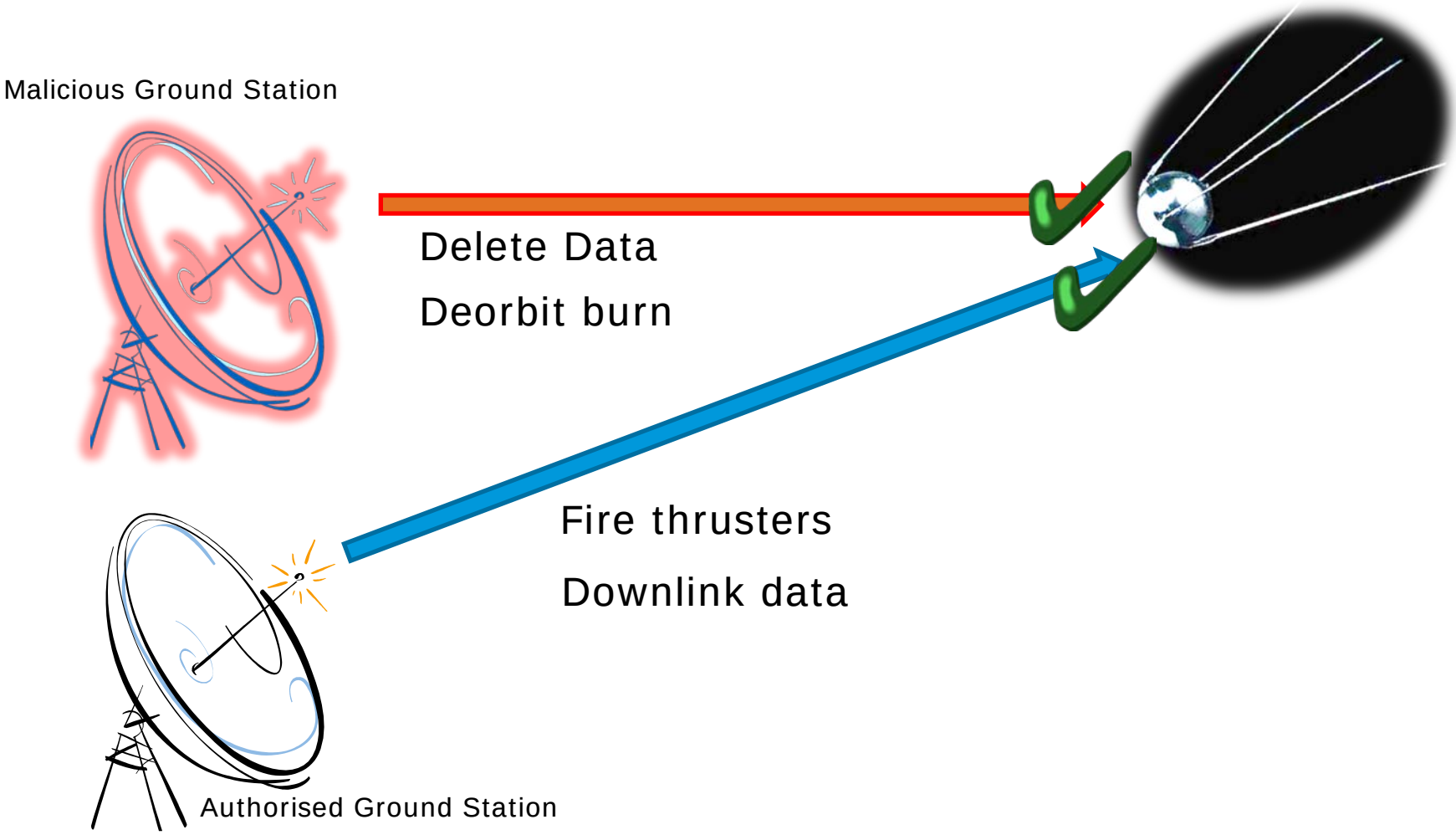
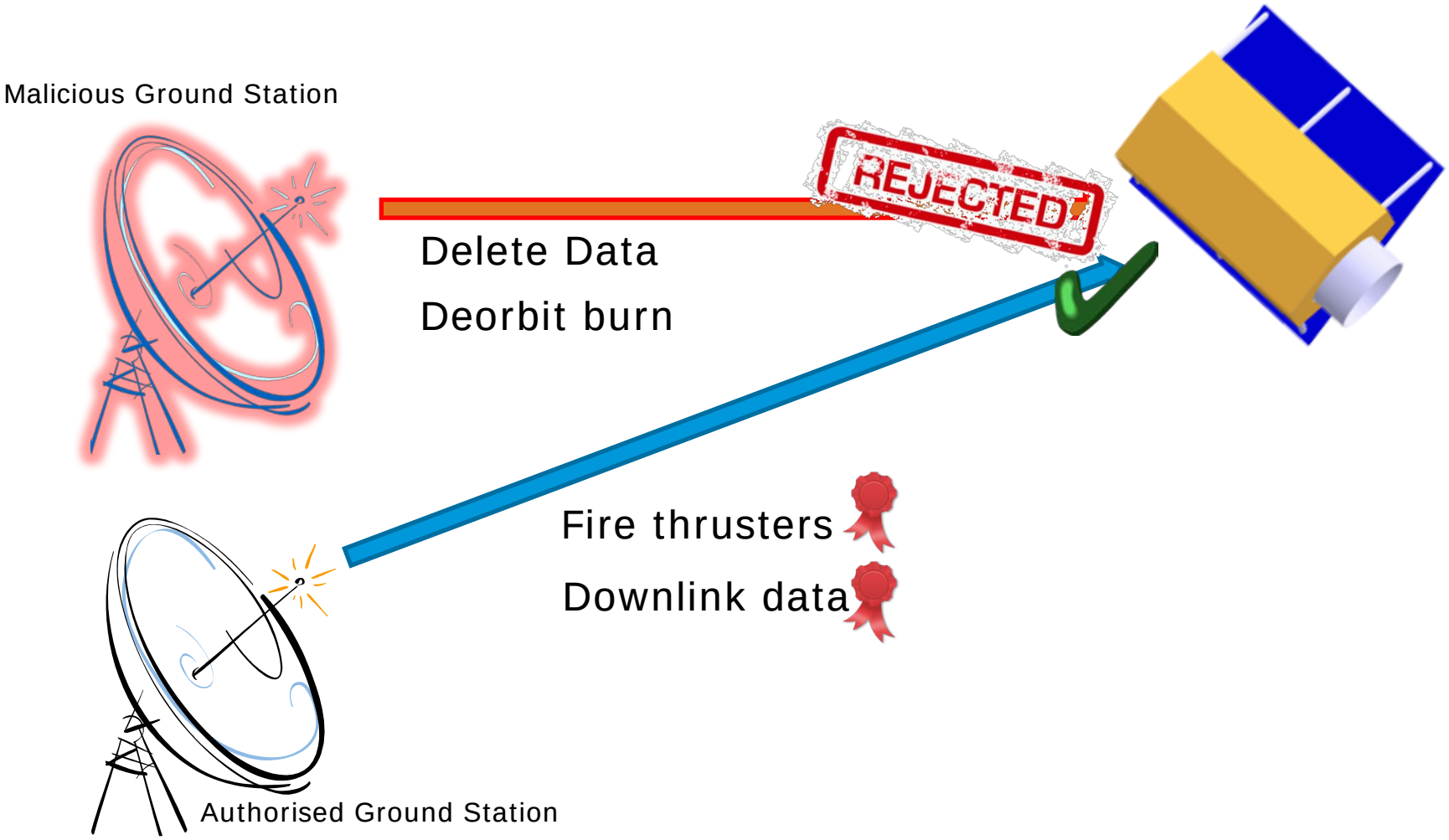
Preparing future Mission Data Systems for Secure Space Communications

M Koller
GSAW 2012
28 Feb 2012

How things started

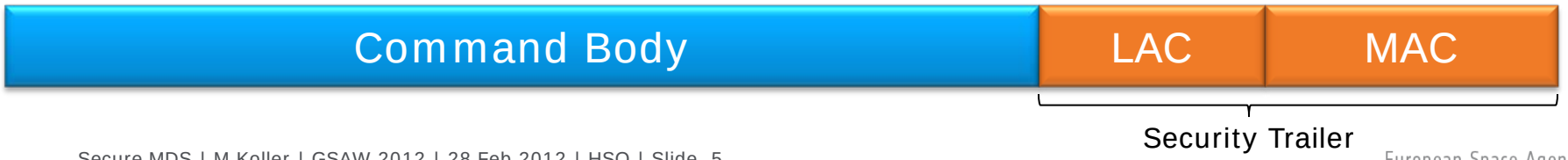


What we want to achieve



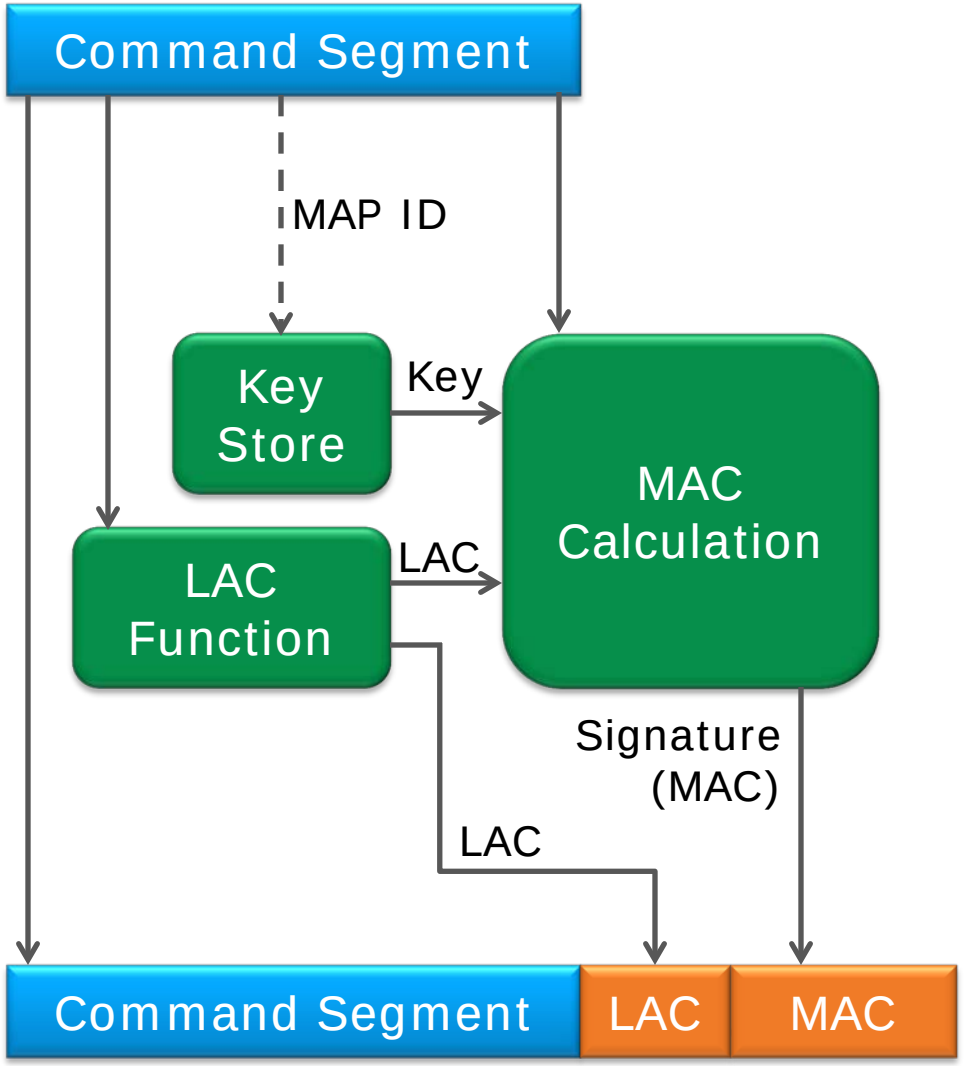
Telecommand Authentication

- Mitigation against Command spoofing/forging
- Elements:
  - Inclusion of Message Authentication Code (MAC)
    - Generated by encryption of the hash of the command and LAC with secret cryptographic key
    - Ensures that commands originate from trusted entities
  - Inclusion of Logical Authentication Counter (LAC)
    - Anti-replay protection
    - Authenticated with the command body
    - Prevents recording and replay of authenticated commands



Authentication Process

- Security enhancements to CCSDS Packet protocol
- Authentication processing located between data-link and segmentation layer
  - SLE service remain untouched
  - Complete transparency to all involved entities
  - Different keys depending on Multiplexer Access Points (MAP)

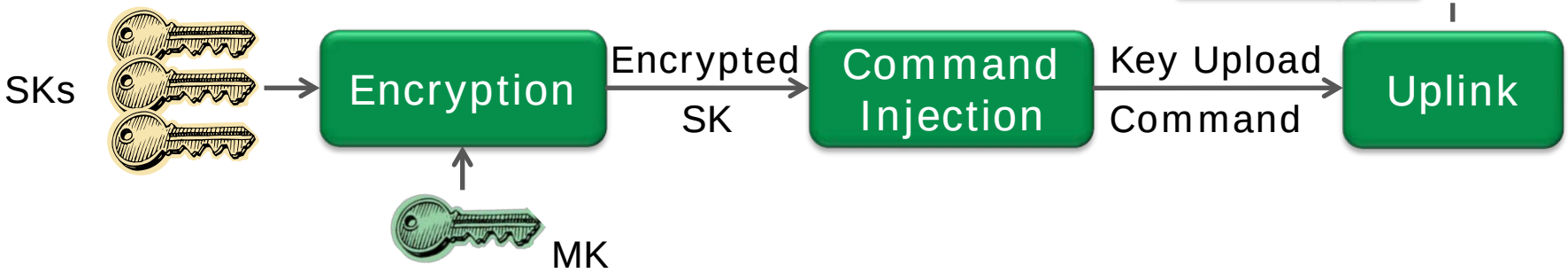


Challenge: Key management

- Generation, Distribution, and Synchronization of Cryptographic Keys to support primary security functions
- Mandatory but non-trivial: secure key distribution via insecure channel
- Key management mechanisms:
    - Static: pre-installation of keys on spacecraft before launch
    - Dynamic: exchange keys in flight
    - Possibility to use both mechanisms

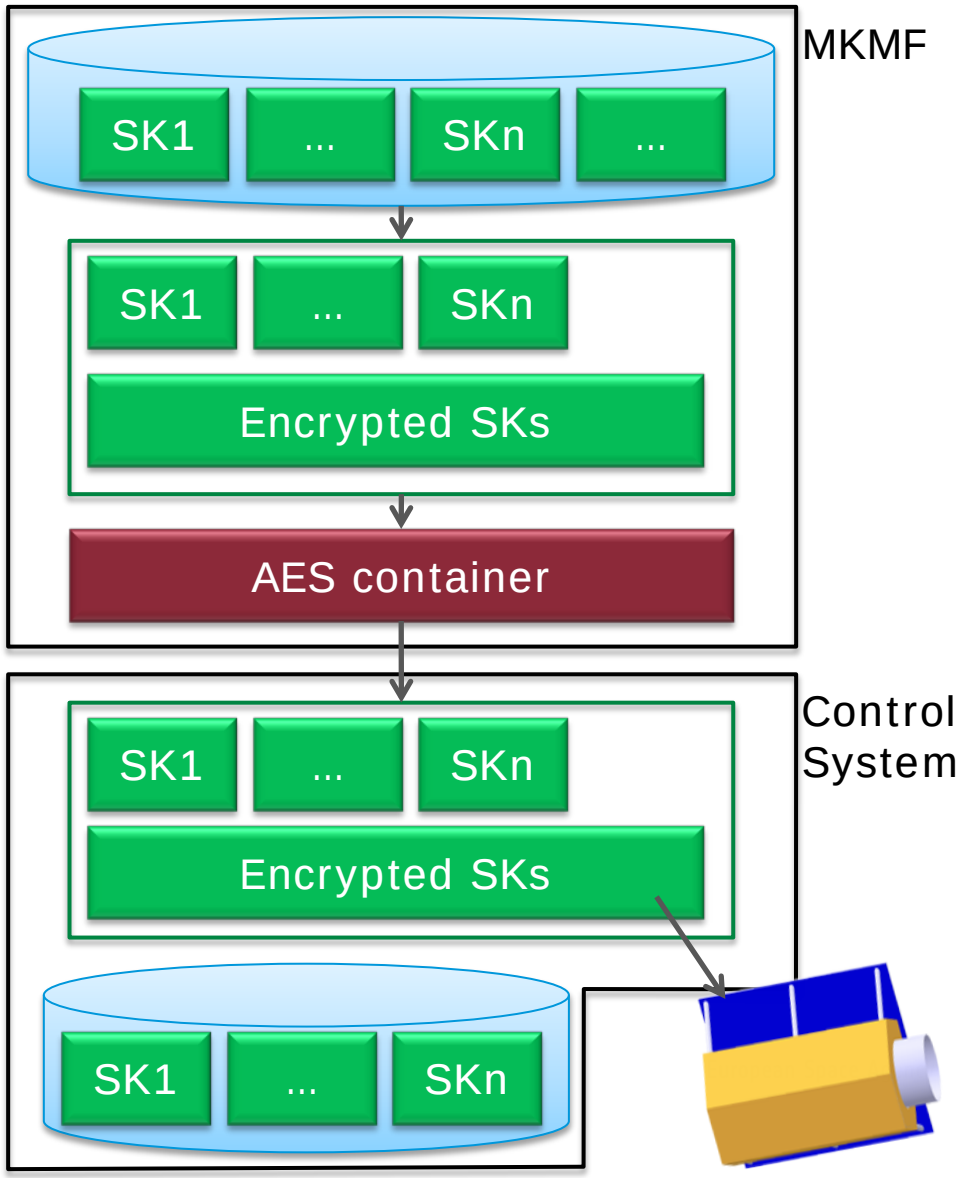
Key Management: GMES Sentinel

- Two level key hierarchy
  - Master Keys (MK)
    - Pre-installed on spacecraft
    - Used for uplink of Session Keys
  - Session Keys (SK)
    - Periodically uplinked to spacecraft
    - Used for authenticated commanding



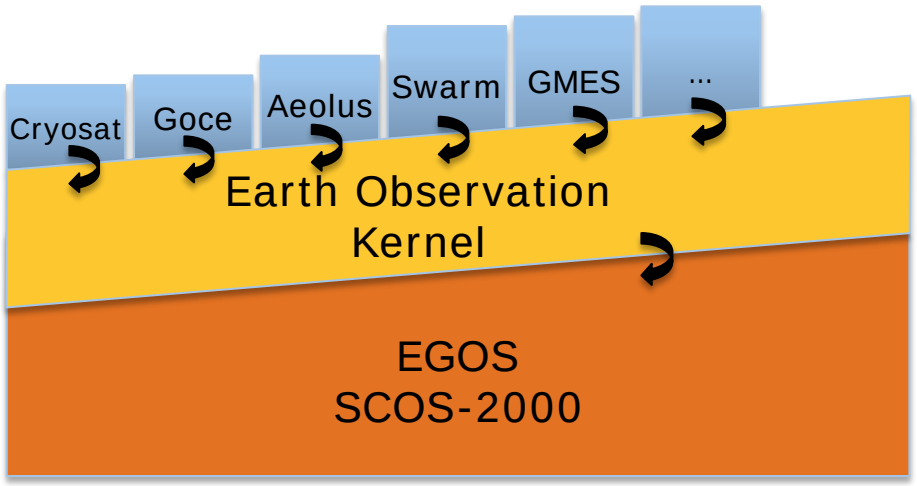
Master Key Management Facility (MKMF)

- Manage and generate Master Keys and Session Keys
- Key Generation using a True Random Number Generator
- Management of all cryptographic keys
- Preparation of Session Keys (SK) for uplink
- Multi-Mission support
- Secure end-to-end communication with key receivers
- Completely isolated system



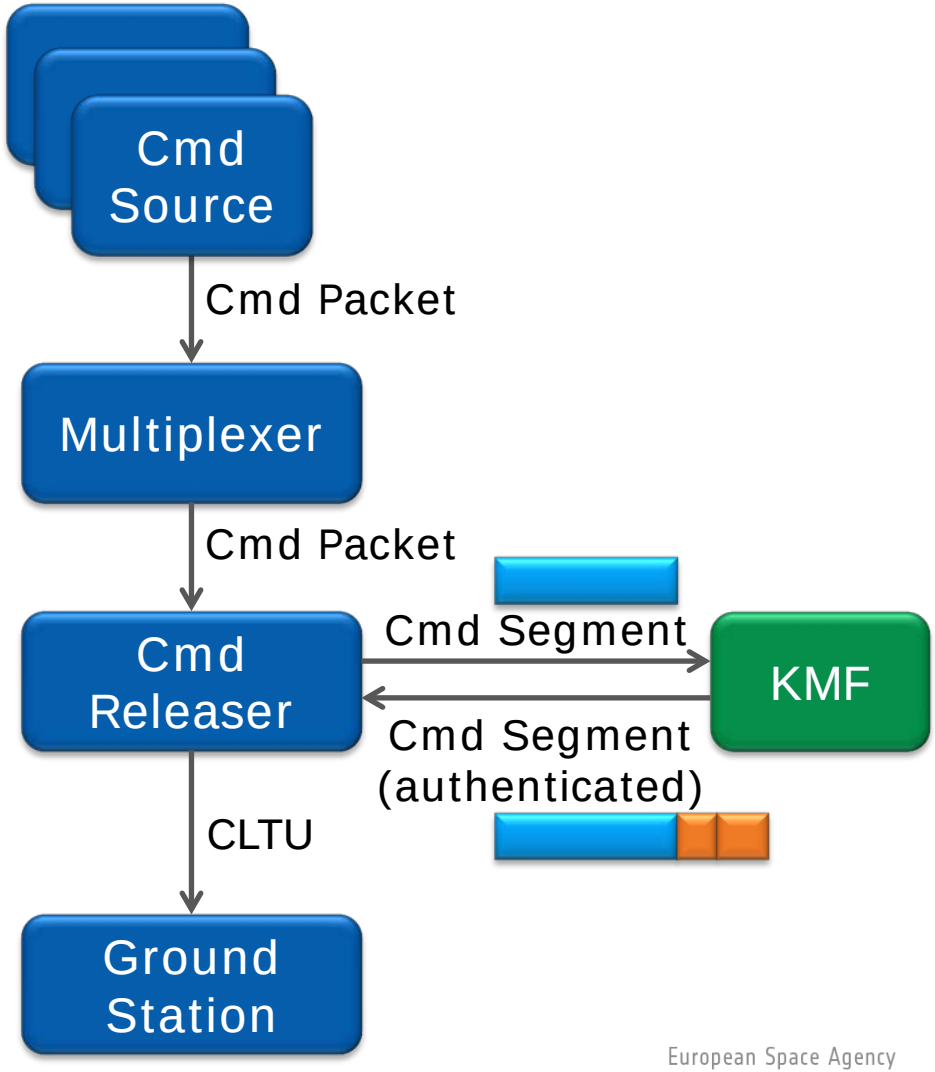
Reuse of existing infrastructure

- Common System kernel for Ground Systems
- Potentially using a Family Kernel
- Requirements definition as delta to underlying systems
- Feedback of new generic functionality for future missions



Adding authentication to Mission Data Systems

- Keep changes to infrastructure minimal
- Mission Control System
  - New “Key Management Facility” (KMF)
  - Routing of created segments through KMF
  - Routing dependent on MAP ID and commanding mode
- Operational Simulator
  - Upgrades to Data Handling System



Wrap Up

- Need for command authentication
- Authentication between data-link and segmentation layer by using Message Authentication Codes and Logical Authentication Counters
- Addressing key management issues by using dual approach (static and dynamic keys)
- Inclusion into existing infrastructure is possible in a minimal invasive way

- Future steps
    - Inclusion of command encryption
    - Inclusion of communication security on the telemetry channel

Any questions?

Preparing future Mission Data Systems for Secure Space Communications

Michael Koller
GSAW 2012
28 Feb 2012