OreSat0 OTA Protocols
http://oresat.org/pub/OreSat0_ota_protocols.pdf
11-Aug-2020

Note:
This is a preliminary document for the most part because the OreSat software development team is currently working on this aspect of the project.
11-Aug-2020

- Authentication [IARU 7.7 and 8.5]

A general description of any cipher system

OreSat uses a mechanism of *authentication of telecommand frames to be acted on* rather than complete message encryption. Only telecommand messages that successfully pass the authentication process will be invoked by the CPU. Because only the invocation of telecommand messages need to be restricted, and there is no sensitive information in the commands themselves, this is a more optimal mechanism of protection. This means that OreSat's ground station control will not encrypt any data up (or down) from the satellite, allowing complete transparency into what is being performed. This mechanism reduces the computational work required by the satellite's CPU reducing power requirement. The authentication algorithms used are in the open source and are vetted by security professionals around the world providing a more safe and reliable code correctness proving process. The mechanism employed is derived from the CCSDS recommendations Security Architecture for Space Data Systems.

See:
https://public.ccsds.org/Pubs/351x0m1.pdf

- Telemetry format [IARU 8.5]

Transmission formats

OreSat over the air (OTA) protocols:

- CW Telemetry Beacon Frame
  - http://oresat.org/pub/CW_Telemetry_Beacon.pdf
- APRS Telemetry Beacon Frame
  - http://oresat.org/pub/APRS_Telemetry_Beacon.pdf
- Engineering Uplink (CCSDS)
- Engineering Downlink (CCSDS)
  - http://oresat.org/pub/engineering_data_link.pdf