Key lifecycle management

Cyber adversaries follow various malicious strategies in order to get to sensitive data. Typically, some approaches count on gathering possibly interesting encrypted traffic for future brute-force “decryption” by a quantum computer. Others do not seek to brute-force their way into encrypted traffic since on today's commodity HW such a task is too expensive. Rather than that, cyber-criminals target poorly secured encryption key storage and simply decrypt harvested data.

How key lifecycle management help:

Key lifecycle management is a cornerstone of a responsible, resilient, and sustainable encryption strategy. Being successful in maintaining confidentiality, integrity, and availability is not just about “the strongest” encryption algorithm. It is about an entire process starting with the way encryption keys are generated, stored, handled, and distributed. Key lifecycle management implements vital processes allowing companies to safely maintain encryption of data at rest in ground stations (and satellite payloads) or in motion while being transferred.

How it works:

Various ground-station services access CORAC KeyMaster REST API to request cryptographic services while encryption keys (the most important part of the encryption process) are safely stored in dedicated storage with strong access controls. Examples of endpoints are as follows:

```
GET /keys/get_secret
GET /keys/get_key_pair
POST /keys/upload_pub_key
```

CORAC KeyMaster crypto API offers multiple services such as key generation, digital signing, HMAC signing, data encryption, and many more.