SYMMETRIC KEY MANAGEMENT

「共通鍵管理」

Magenta Book
CCSDS 354.0-M-1
発行月：2023年12月
ISO －

【概要】

本推奨実践規範は、CCSDSの共通暗号鍵管理の実施にあたり、鍵の種類、ライフサイクルおよび、管理手順を規定する。

【内容】

暗号化は、スペースリンク通信において、送信された情報の不正な開示からの保護、改ざんの検出および、地上または宇宙エンティティの身元認証（機密性、完全性、真正性の提供）に使用される。暗号化技術ではライフサイクルにおいて、鍵管理フレームワークにて管理および、保護された暗号鍵が使用される。

共通鍵暗号方式は、ポイント・ツー・ポイント通信を用いる宇宙ミッション通信セキュリティで、複雑さ、計算量において公開鍵暗号方式に比べ優位であることから推奨される方式である。また、本書に記載している仕様は、SDLSプロトコル[参考：Space Data Link Security Protocol (CCSDS 355.0-B-2)] などのセキュリティプロトコルにも実装可能である。

第3章では、暗号鍵をマスター鍵とセッション鍵の2種類に分けて、それぞれの役割について定義している。マスター鍵は、Over-The-Air-Rekeying（無線環境での鍵更新）もしくはセッション鍵の生成に対する、暗号化あるいは認証付き暗号化を行うために利用される。セッション鍵は、保護されたデータに対する、認証、暗号化、認証付き暗号化を行うために利用される。また、暗号鍵には状態モデルがあり、ライフサイクルとして必ずいずれかの状態に属する。図1は、鍵の状態モデルと遷移を示す。

第4章では、暗号通信を実現するために必要な鍵管理サービス（鍵の活性化、非活性化、破壊、検証、無線環境での鍵更新、抹消、セッション鍵生成、無効化、有効化）を定義している。具体的な実装方法については、対象となるセキュリティプロトコル特有となるため、本章では抽象的な記述としている。

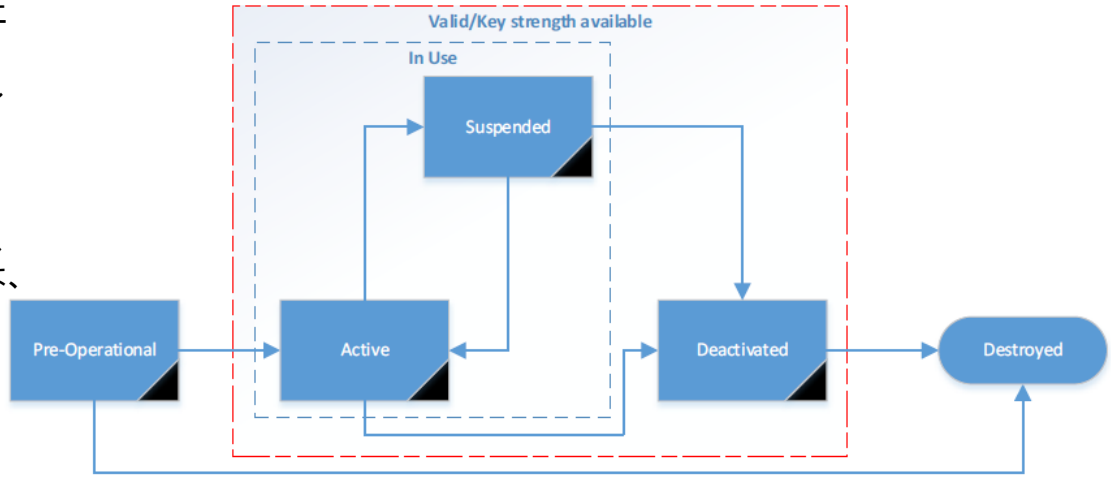

図1: 鍵の状態モデルと遷移

各国宇宙機関およびJAXAの動向
新規文書につき、現在情報を収集中。