요약

물리적보안
자가시험
생명주기보장

물리적보안

모듈 내용물에 대한 비인가된 물리적 접근을 제한하고 설치 시 모듈의 비인가된 사용이나 변경(모듈 전체 내용물 교체 포함)을 방어하기 위하여 물리적 보안 메커니즘을 사용해야함

암호경계 내의 모든 하드웨어, 소프트웨어, 펌웨어, 데이터 구성 요소 및 SSP를 보호해야함

자가시험

성공 또는 실패가 암호모듈 내에서만 결정되고 암호모듈은 함수 또는 알고리즘과 관련된 자가시험이 반복 수행되어 성공적으로 통과될 때까지 자가시험이 실패한 함수와 알고리즘에 관련된 어떠한 기능도 사용하지 않아야 한다.

정상 동작 전과 암호알고리즘, 키쌍 일치성, 소프트웨어/펌웨어 로드, 수동 주입, 조건부 우회 및 핵심 기능시험 등의 상황에서 자가시험을 진행한다.

생명주기보장

암호모듈이 벤더가 의해 적절하게 사용되고 운영되고 있는 지를 보장한다.

형상 관리, 설계, 유한상태모델, 개발, 벤더 시헌, 배포 및 운영, 수명의 종료, 안내서의 항목을 통해 암호 모듈의 개발 및 배포, 운영에 대한 정보를 포함한다.