1. 신재생자료취득장치의 보안 규격

○ 신재생자료취득장치는 X.509 표준 포맷 인증서를 통해 데이터 수집서버와 상호인증을 수행할 수 있어야 한다.

- 신재생자료취득장치는 수집서버 인증서에 대한 유효성 검증을 수행해야 한다.

○ 신재생자료취득장치는 수집서버와의 통신을 위한 어플리케이션 코드, 인증서, 인증서 암호 그리고 신재생자료취득장치에서 취득한 모든 데이터를 암호화하여 저장하여야 한다.

- 암호화에 사용하는 알고리즘은 AES-256-CBC 혹은 그 이상의 보안 수준을 가지는 알고리즘을 사용하여야 한다.

- 암호화에 사용되는 정보는 별도의 하드웨어 보안 모듈(HSM)를 사용하여 암호화 되어야 하다.

○ 신재생자료취득장치는 한국인터넷진흥원 IoT보안인증서비스(IoT-SAP)의 Basic 이상의 등급을 획득[1]하여야 한다.

○ 신재생자료취득장치와 수집서버는 다음의 알고리즘을 적용한 KCMVP 검증필 모듈[2]을 적용하여 TLS 1.2 통신을 수행하여야 하며, 해당 알고리즘 사용에 대한 증빙을 제출할 수 있어야 한다.

- 전자서명 알고리즘 : ECDSA

- 키교환 알고리즘 : ECDHE

- 해시 알고리즘 : SHA-256

- 키 유도 알고리즘 : HMAC-SHA-256

- 난수 발생 알고리즘 : HMAC-DRBG (SHA256) 혹은 HMAC-DRBG

1) 보안인증의 의무적용은 2022년 12월 31일까지 유예한다.

2) KCMVP 검증필 모듈의 의무적용은 2022년 12월 31일까지 유예한다.

(SHA512)

- 암복호화 알고리즘 : ARIA-128-CBC

2. 신재생자료취득장치의 통신 규격

○ 신재생자료취득장치는 TLS1.2 상에서 MQTT 5버전으로 데이터 수집 서버와 통신한다.

- MQTT 접속 계정은 신재생자료취득장치 신고 후 거래소에서 발급하여 전달한다.

○ 신재생자료취득장치는 매 1분 간격으로 데이터를 전송하고, 시스템 관리자의 요청에 따라 1분 보다 작은 시간 단위로 전송 주기를 변경할 수 있어야 한다.

- 1분 단위 이내 데이터 전송을 위하여 월 최소 1GB 이상의 통신 용량을 확보하여야 한다.

○ 신재생 자료 송신을 위한 토픽과 제어 명령 수신을 위한 토픽 정보는 신재생자료취득장치 신고 후 거래소에서 발급하여 제공한다.

- 자료 전송 및 제어명령 전달을 위한 데이터 형식은 별도의 문서로 제공한다.

3. 신재생자료취득장치의 데이터 수집 규격

○ 신재생자료취득장치는 발전소로부터 1분 이내의 단위로 데이터를 수집하여야 하며, 수집된 데이터는 1개월 이상 보관할 수 있어야 한다.

○ 신재생자료취득장치는 데이터 보관을 위하여 최소 200MB 이상의 저장 공간을 확보하여야 한다.