IoT platform security enhancements

IT 보안팀 조성규

2016. 7. 14.

R.A & Crypto lib.

- **주요 이슈**
  - R.A issue
    - Privacy CA와 단말 통신 간에 오류 확인 중
      - ID+공개키를 PCA로 보내고, Cert. 생성 후 리턴하였는데 리턴받은 해당 cert 값의 verification 에서 오류가 발생 중
        - 원인 확인 중 - 이번 주 (7.15.) 중에 완료가능할 것으로 보임
      - 이후의 기술적 난제는 measurements list 송수신 과정, 나머지는 큰 technical risk 작은 편
  - Crypto lib. issue
    - 현재 resource 를 R.A쪽에 집중 중
    - 해당 기능은 기본적으로 tpm 에서 지원하므로, 구현은 크게 어렵지 않을 것으로 판단됨
    - 기본적인 spec. 에 대해서 차주(7.22.) 까지 정의 완료 예정