Minutes of conf call on October 27th, 2011

of Device Security group

Editor: Marc Vauclair (NXP)

Participants:

* Marc Vauclair - NXP
* Gio Gallo – Sensus
* René Struik
* Rohit Khera - S&C
* Dave Mitton – Ambien
* Chris (?Gorog?)

Agenda:

* Rene: what kind of crypto to look at for the specification
* Rohit: going over the plan for the deliverables and the assignments

The second item was not covered during the call due to lack of time.

Minutes:

* What kind of crypto to look at for the specification?
  + during the call we discussed at length the basis cryptographic primitives on which we may build our specification
  + requirements:
    - limit certificates size
    - foresee extensibility and upgradeability
  + A TRNG is in the make at NIST
    - to see how it relates to the AIS31 from Germany
  + SCADA DNP: RSA is the only one specified
  + It would be nice to have 4 crypto suites slots:
    - symmetric only (PSK, Pre-shared secret)
    - asymmetric with ECC
    - asymmetric with RSA
    - one open slot for replacement of one of the 3 above in case of an issue with one of them.
  + We discusses the approach of NIST vs BSI for the key sizes
  + Action: recover the BSI document with key size recommendations
  + Action: recover the French equivalent document with key size recommendations
  + Action: check 192 key size against the current NIST recommendations.