Minutes of conf call on April 18th, 2012   
of Device Security group

Editor: Wim Nuyts (NXP) (updated by Marc Vauclair (NXP))

Participants:

* David M [Ambient Corp]
* Shrinath E [Infineon]
* Rohit K [S&C]
* Marc V [NXP]
* Wim N [NXP]
* Chris G [Deloitte]

Minutes of the meeting:

* Shrinath suggests to push the topic leaders to contribute.
  + Progress is rather slow, we should try to address the open sections…
* Shrinath has provided a reference (link) to an interesting draft document about key management (recommendation for NIST)

|  |
| --- |
| Apr. 13, 2012  **SP 800-130**  **DRAFT A Framework for Designing Cryptographic Key Management Systems**  NIST requests comments on SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*. This is a revision of the document that was provided for public comment in June 2010. Comments are requested by **July 30, 2012** and should be sent to [ckmsdesignframework@nist.gov](mailto:ckmsdesignframework@nist.gov?Subject=Comments%20Draft%20SP%20800-130), with "Comments on SP 800-130" in the subject line. Another document, SP 800-152, which provides a basic profile of this framework document for the Federal government, will be available for initial comment later this year.  <http://csrc.nist.gov/publications/PubsDrafts.html> |

* Other topics?
  + Any review feedbacks about James/Shrinath?
    - No new feedback received.
  + Rohit will forward the presentation that he gave at the OpenSG meeting. (Editor: Document provided by Rohit put here: <http://osgug.ucaiug.org/utilisec/embedded/Shared%20Documents/Device%20Security/Meeting%20Minutes/KnoxVille2012_Embedded%20Sec%20Update.ppt>)
  + Marc will check if LiveMeeting is an option for reviewing documentation during the calls.
    - Shrinath agrees but points out that we should add new sections to proceed faster.
    - Action point: RNG (Wim)/device identity & authentication (Marc)/key management(Shrinath)/compliance & certification (Mike) /secure protocols (James) will be asked to update the relevant sections.
    - Cipher section needs to be done over again?
      * 2 options: leave everything open (all possible certified ciphers) or define cipher suites
        + Cipher suites preferred to avoid chaos
        + E.g. NIST suite B as example

**Action point for all:** look into suite B to see if this is acceptable as recommendation.

Rene S. can join? (Marc will check)

Marc will send out the meetings minutes early

* + We will provide some material as response to Mike’s idea of convicing the need for security to e.g. utilities (as discussed in previous meeting)