TEEP
Trusted Execution Environment Protocol

IETF BoF Meeting

March 28, 2017 Session II

Nancy Cam-Winget and Tero Kivinen, Co-Chairs

Note Well

- **Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution".** Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - **Any IETF mailing list**, including the IETF list itself, any **working group** or design team list, or any other list functioning under IETF auspices
  - Any **IETF working group or portion thereof**
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of **RFC 5378** and **RFC 3979** (updated by **RFC 4879**).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Problem Statement and Background Info on Trusted Execution Environments (15 minutes -- Hannes)
- ARM-based TEE Implementation Example (5 minutes -- Hannes)
- Intel-based TEE Implementation Example (5 minutes – David/remote)
- Use Cases (15 minutes -- Dapeng)
- Architecture (20 minutes -- Ming)
- Charter Discussion (Chairs -- 30 minutes)

Charter Discussion

- IETF to define protocols for Provisioning TEE App
    - Downloading from TSM to TEE
    - Authentication of TEE to TSM
    - TSM Authorize request for TEE Provisioning
- Does charter include “Normal” App verification of TEE (and) TEE App?

Charter Focus (Poll)

- Does the group understand the work to be done?
- Is this work something to be solved?
- Should the IETF provide the solution?