

# SUIT BoF

## Software Updates for Internet of Things

Co-Chairs: Dave Waltermire, Russ Housley and Dave Thaler

Monday, November 13, 2017 – IETF 100 Singapore

# 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

1. Agenda bashing, Logistics -- Chairs (5 min)
2. Review of proposed charter text -- Chairs (10 mins)
3. Charter discussion -- Chairs (45 mins)
4. Discussion of new work items (20 mins) – Time permitting
  - Hannes Tschofenig
    - draft-moran-suit-architecture
    - draft-moran-suit-manifest
  - Suhas Nandakumar
    - draft-nandakumar-suit-secfu-requirements
    - draft-nandakumar-suit-secfu-solution-arch
5. Review of milestones & wrap up -- Chairs (10 minutes)

# Logistics

- Please sign the blue sheets

## Volunteers:

- Jabber scribe: Stephen Banghart
  - Jabber: xmpp:suit@jabber.ietf.org?join
  - MeetEcho: <http://www.meetecho.com/ietf100/suit>
- Need two note takers
  - Etherpad: <http://etherpad.tools.ietf.org/p/notes-ietf-100-suit>

Thank you for helping!

# Charter review – Current status

- Lots of charter discussion on the mailing list since the IETF 99 side meeting
- Charter has been through internal review - initial IESG and IAB review
- Currently in external review – scheduled for 11/30/2017 telechat

# Review of Charter text

Things to consider during this discussion:

- Is the charter text clear?
- Does it capture the work to be done?
- What can we do quickly?

Out of scope:

- This effort does not intend to define a transport protocol.

# Trusted Execution Environment Provisioning (TEEP) BoF

- Date: Wednesday Nov. 15, 2017
- Time: 13:30-15:00
- Room: Collyer
- **Description:** Today, hardware-enforced Trusted Execution Environments (TEEs) such as TrustZone and SGX are found in many smart phones, tablets, wearables, home routers, set-top boxes, etc., but proprietary protocols are used to securely provision them with software and credentials. This BoF will discuss forming a WG to standardize protocol(s) for such provisioning.
- Draft charter: <https://datatracker.ietf.org/doc/charter-ietf-teep/>

# Relationship between SUIT and TEEP

- In *currently* proposed charters (subject to change):
- TEEP focuses on installation of code into a Trusted Execution Environment (whether
- for IoT or not), whereas SUIT focuses on installation of code on an IoT device (whether in a TEE or not)
- TEEP focuses more on initial provisioning of code the first time, whereas SUIT focuses more on subsequent updates to already-provisioned code
- TEEP focuses more on trusted "apps" after boot, whereas SUIT focuses more on "firmware" for boot

What SHOULD the work split be?

What changes should be made to the charter to reflect this relationship?



# Serialization Format

- Single or multiple formats?
  - Fewer/One is better
- Align capabilities already in use on the device
  - e.g., is the encoding used as part of its function?
- The number of formats affects code size
  - e.g., class 1 devices have 10KiB RAM, 100KiB flash
  - Multiple decoders increase code size
- Interoperability
  - Tool chains and distribution methods may need to read the manifest
- Other concerns?
- How do we strike a balance given these concerns?

# Charter Discussion – Other Questions

1. Do we work on an update to RFC 4108bis?
  - Or leave as-is and work on a new approach?
  - What should this work entail?
2. To what extent does this work need to address post-quantum resistance?
3. Are there other SDOs that we should coordinate with (e.g., TCG, GP, LWM2M)?
4. Other concerns?

# Milestone Discussion

Do these milestones make sense? Are they achievable?

Nov 2018 - Submit "Manifest Format" to the IESG for publication as a Proposed Standard.

Nov 2018 - Submit RFC 4108bis document to the IESG for publication as a Proposed Standard.

Jun 2018 - Calendar item: Release first IoT OS implementation of firmware update mechanisms as open source.

Apr 2018 - Calendar item: Release first version of manifest test tools as open source.

Mar 2018- Calendar item: Release initial version of the manifest creation tools as open source.

Jan 2018 - Adopt "Architecture" to the IESG for publication as an Informational RFC.

Dec 2017- Adopt "Manifest Format" specification as WG item.

Dec 2017 - Adopt "Architecture" document as WG item.

Dec 2017 - Adopt RFC 4108bis document as WG item.

# Next Steps

- This week - Complete charter for external review
- Complete external review
  - scheduled for 11/30/2017 IESG Telechat
- If chartered, when will we next meet?
  - IETF 101?
  - Virtual interim?
- Other considerations?